TEXAS
Department of Family
and Protective Services

DFPS Office of Information Security

Information Security and Privacy Controls Catalog

INTRODUCTION

The Texas Department of Family and Protective Services (DFPS) Office of Information Security (OIS) Security and Privacy Controls Catalog establishes the minimum standards and controls for information security in accordance with the state's Information Security Standards for State Agencies found in Title 1, Chapter 202, Texas Administrative Code (TAC 202).

The purpose of this Controls Catalog is to provide DFPS information owners, custodians and users with specific guidance for implementing security controls conforming to security control standards currently required in the Texas Department of Information Resources (DIR) Security Control Standards Catalog, Version 1.3.

Each control group is organized under its two-letter group identification code and title and adopts the numbering format of the DIR Security Control Standards Catalog.

AUDIENCE

This Catalog applies to all information systems and associated entities that process, store, or maintain DFPS data. All DFPS information owners and custodians should read and understand those portions of this Catalog that apply to the systems for which they are responsible.

While all users of DFPS information systems assets should be aware of security controls as adopted by DFPS Office of Information Security, primary users of this document are the information custodians of IT operations, system and database administrators, application developers, IT support, IT maintenance personnel, and Cybersecurity Analyst.

SCOPE

The intent of the Catalog is to record all security and privacy control requirements with which DFPS systems may be required to comply based on system categorization and data classification.

This catalog applies to all technology assets, including but not limited to systems (including cloud-based systems), networks, servers, operating systems (including virtual machines), databases, and applications.

ABOUT THE CONTROLS CATALOG

The control catalog specifies the minimum information security requirements that state organizations must use to provide the appropriate levels of information security according to risk levels. The control catalog specifies the purpose, levels of risk, implementation overview, and implementation examples for each control activity.

Certain federal programs, such as the Social Security Administration (SSA) and the Federal Bureau of Investigation (FBI) have specific control implementation standards that are required. Each Federal agency has unique data protection regulations and requirements. DFPS systems and our contractors must adhere to the safeguard requirements of the Federal agencies when mandated by a contractor and interconnection agreement.

For more information related to information security requirements for state organizations, refer to Texas Administrative Code (1 TAC 202).

USING THIS CATALOG

Based on National Institute of Standards and Technology (NIST) Special Publication 800-53 revision 5, the Controls Catalog includes requirements derived from state authority, including the Texas Department

of Information Resources (DIR) and state legislation, as well as agency-specific requirements as determined by the DFPS Chief Information Security Officer (CISO) in light of the environment of operations and the agency's security posture.

The intent of the Catalog is to record all security and privacy control requirements with which DFPS systems may be required to comply based on system categorization and data classification.

The DFPS Information Security and Privacy Controls Standards Catalog establishes the minimum requirements for DFPS information security assets. This document is an expansion of the DFPS Information Security Policy requirements.

PUBLICATION

The DFPS Information Security and Privacy Catalog (including all DFPS information security and privacy control requirements, implementation standards, discussion, and references) is maintained by DFPS Office of Information Security. For a Word or Excel version of this Catalog, please e-mail infosec@dfps.texas.gov.

The Catalog was developed from NIST's SP 800-53r5 (released Sept. 2020, updated to r5.1 December 2020) and 800- 53B (October 2020). Titles for controls and enhancements are identical to those in that document though reformatted for readability.

Contact

Questions about this content must be directed to infosec@dfps.texas.gov. Only the DFPS Chief Information Security Officer or their delegate can address questions about this standard.

Appendix A – Catalog Fields

Appendix A provides a view of the control and enhancement format with brief descriptions of source and use.

Note that the Catalog's contents may be combined or excerpted for different subject areas across the agency. Some fields may be combined or omitted depending on need; for example, a single References field on the GRC site contains the same information as the DFPS References, State References, and Federal References fields used in this Catalog.

Appendix B – FBI CJIS CSP to DFPS Control IDs

This table provides a mapping of FBI CJIS CSP requirements to the DFPS controls. This mapping should only be used as a reference when deciding how to implement required security controls set forth in the CJIS Security Policy. The corresponding federal controls are listed for each policy section. The cross-reference is a "best fit" correlation between the CJIS Security Policy controls and the federal controls and may not be exact. Agencies must always meet the requirements in the CJIS Security Policy during audits.

The most recent version of the federal controls can be found on the FBI's web site at this location: https://www.fbi.gov/file-repository/cjis_security_policy_v5-9_20200601.pdf/view

Appendix C – Detailed Change Log

This table provides a list of changes made to individual controls and enhancements since the last publication.

Crosswalks and Mappings

The DFPS Office of Information Security has mappings of the NIST Cybersecurity Framework (CSF) and NIST Privacy Framework (PF) to NIST Special Publication (SP) 800-53, Revision 5 which is available upon request in Microsoft Excel Format.

Request for these mappings can be directed to infosec@dfps.texas.gov

Document History

Version	Date	Prepared/Updated By	Brief Description of Change
v1.0	02/01/2022	Jennifer Bush DFPS Cybersecurity Operations Manager	Initial Catalog release, published to DFPS Public Facing website, Internal GRC site and uploaded to DIR.

Authorized by: Jennifer Bush, Acting DFPS Chief Information Security Officer

Effective Date: 06/01/2022

Date of Last Revision: 02/01/2022

Authorized Signature:

TABLE OF CONTENTS

(AC) ACCESS CONTROL

The DFPS organization requires limited access to applications, servers, databases, and network devices in the DFPS environment. Access is limited to authorized users, processes acting on behalf of authorized users, or devices. Authorized users are further limited to the types of transactions and functions that they are permitted to exercise.

The AC Control Family consists of security requirements detailing system logging. This includes who has access to what assets and reporting capabilities like account management, system privileges, and remote access logging to determine when users have access to the system and their level of access.

The intended audience for this Control includes, but is not limited to, information resource owners and custodians. Information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented.

AC-01: ACCESS CONTROL **POLICY AND PROCEDURES**	
Priority: P1	
Baseline(s): Low, Moderate, High	Overlay(s): CJIS, DIR

CONTROL REQUIREMENTS

a. Develop, document, and disseminate to appropriate personnel:
   1. Organization-level access control policy that:
      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the access control policy and the associated access controls;
b. Designate a senior management official as defined in the access control policy to manage the development, documentation, and dissemination of the access control policy and procedures; and
c. Review and update the current access control:
   1. Policy every year and following major changes to legislation or security requirements; and
   2. Procedures every year and following major changes to legislation or security requirements.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - Create, distribute, and implement an account management policy which defines the rules for establishing user identity, administering user accounts, and establishing and monitoring user access to information resources. [Source: DIR Control Standards Catalog AC-1]

Std.02 - The Information Security Officer is responsible for:

a. Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks;

b. Providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities under 1 TAC 202; and

c. Developing and recommending policies and establishing procedures and practices, in cooperation with the agency Information Resources Manager, information-owners and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, or disclosure. [Source: 1 TAC 202.21(b)(3, 5, 8)]

SUPPLEMENTAL GUIDANCE

Access control policy and procedures address the controls in the AC family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of access control policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies reflecting the complex nature of organizations.

Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to access control policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; OP-2126 Account Management Policy **State:** DIR Security Control Standards Catalog **Federal:** OMB A-130; NIST SP 800-12, 800-30, 800-39, 800-100; NIST IR 7874; CJIS CSP v5.9 Section 5.13.1	IA-1, PM-9, PM-24, PS-8, SI-12

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy and procedures; system security plan, other relevant documents, or records. Examine: Verify that the access control procedures are consistent with access control policy.

Examine: Verify that the access control procedures address all areas identified in the access control policy and address achieving policy-compliant implementations of all associated access control controls.

Examine: Examine document transmission logs or audit logs or records to confirm that the access control policy and procedures have been disseminated or otherwise made available.

Examine: Examine policy and procedure documents to verify that responsible personnel are required to review the access control policy and procedures within the required timeframe and to update as necessary. Examine document changes, document revision records, after-action reports, etc., to ensure reviews were conducted.

Interview: Organizational personnel with access control responsibilities. Verify that personnel:

1. Confirm their respective roles with Access Control policy;
2. Know of and understand Access Control policy and procedures; and
3. Are responsible for reviewing and updating Access Control policy and procedures no less often than required.

Priority: P1	
Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization employs automated mechanisms to support the management of information system accounts.

CONTROL IMPLEMENTATION STANDARDS

The use of automated mechanisms can include, for example: using email or text messaging to automatically notify account managers when users are terminated, transferred, or change their role; using the information system to monitor account usage; and using telephonic notification to report atypical information system account usage.

AGENCY IMPLEMENTATION

Std.01 – DFPS employs automated mechanisms to support the management of information system accounts. The electronic Move, Add, Change, and Remove (eMAC) system is a proprietary tool for account management that uses automated mechanisms from the system include internal system functions and email notifications.

Std.02 - The agency uses additional automated system account management tools to monitor system account usage and report atypical system account usage through email notification directly to the DFPS Office of Information Security.

SUPPLEMENTAL GUIDANCE

The use of automated mechanisms can include, for example: using email or text messaging to automatically notify account managers when users are terminated or transferred; using the information system to monitor account usage; and using telephonic notification to report atypical system account usage.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Account Management Policy. **State:** DIR Security Control Standards Catalog **Federal:** NIST SP 800-12, 800-30, 800-39, 800-100; NIST IR 7874; CJIS CSP v5.9 Section 5.13.1	AC-3, AC-5, AC-6, AC-17, AC-18, AC-20, AC-24, AU-2, AU-12, CM-5, IA-2, IA-4, IA-5, IA-8, MA-3, MA-5, PE-2, PL-4, PS-2, PS-4, PS-5, PS-7, PT-2, PT-3, SC-7, SC-12, SC-13, SC-37.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures for addressing account management; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

Interview: Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security with information security responsibilities; system developers.

Test: Automated mechanisms for implementing account management functions

AC-02 (01) AUTOMATED SYSTEM ACCOUNT MANAGEMENT

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

Support the management of system accounts using automated mechanisms as defined in System Security Plans (SSPs).

AGENCY IMPLEMENTATION STANDARDS

Std.01 - DFPS employs automated mechanisms to support the management of information system accounts.

Std.02 - The electronic Move, Add, Change, and Remove (eMAC) system is a proprietary online tool for DFPS staff to request to DFPS Information Technology Services (ITS) for an account to be created. Automated mechanisms from the system include internal system functions and email notifications.

SUPPLEMENTAL GUIDANCE

All accounts are deactivated, disabled, or appropriately changed if the account privileges are no longer appropriate or necessary for the user's job functions or level of privilege. A user account may be deactivated, modified, or disabled if it is found that the account is compromised or misused.

DFPS Information Technology Services (ITS) disables all accounts that have not been accessed for 30 days. ITS archives employee accounts that have not been accessed for 90 days. Management of temporary and emergency accounts includes the disabling of such accounts automatically after the predefined time period rather than at the convenience of the network security administrator. Automatic disabling of accounts provides a more consistent implementation.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; OP-2126 Account Management Policy **State:** DIR Security Control Standards Catalog **Federal:** NIST SP 800-12, 800-30, 800-39, 800-100; NIST IR 7874; CJIS CSP v5.9 Section 5.13.1	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System security plan; information system design documentation; information system configuration settings and associated documentation; information system-generated list of active accounts; information system audit records; and other relevant documents or records.

Examine: Information system demonstrates automated mechanisms are used to automatically disable temporary accounts and emergency accounts in defined time period.

Test: Automated mechanisms implementing account management functions. Review audit log to verify that the proper account management actions were taken and were recorded by automated mechanism.

AC-02(02): REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

Automatically disable temporary and emergency accounts after the period specified in Std.01.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - All accounts are deactivated, disabled, or appropriately changed if the account privileges are no longer appropriate or necessary for the user's job functions or level of privilege. A user account may be deactivated, modified, or disabled if it is found that the account is compromised or misused.

Std.02 - DFPS Information Technology Services (ITS) disables all accounts that have not been accessed for 30 days. ITS archives employee accounts that have not been accessed for 90 days

SUPPLEMENTAL GUIDANCE

Management of temporary and emergency accounts includes the removal or disabling of such accounts automatically after a predefined time period rather than at the convenience of the system administrator. Automatic removal or disabling of accounts provides a more consistent implementation.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Account Management Policy **State:** DIR Security Control Standards Catalog **Federal:** NIST SP 800-162, 800-178, 800-192; FBI CJIS CSP v5.9	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures for addressing account management; system design documentation; system configuration settings and associated documentation; system-generated list of temporary accounts removed and/or disabled; system-generated list of emergency accounts removed and/or disabled; system audit records; system security plan; other relevant documents or records

Interview: Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security with information security responsibilities; system developers.

Test: Automated mechanisms for implementing account management functions.

AC-02(03): DISABLE INACTIVE ACCOUNTS

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

Automatically disable temporary and emergency accounts after the period specified in Std.01.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - All accounts are deactivated, disabled, or appropriately changed if the account privileges are no longer appropriate or necessary for the user's job functions or level of privilege. A user account may be deactivated, modified, or disabled if it is found that the account is compromised or misused.

Std.02 - DFPS Information Technology Services (ITS) disables all accounts that have not been accessed for 30 days. ITS archives employee accounts that have not been accessed for 90 days

SUPPLEMENTAL GUIDANCE

Management of temporary and emergency accounts includes the removal or disabling of such accounts automatically after a predefined time period rather than at the convenience of the system administrator. Automatic removal or disabling of accounts provides a more consistent implementation.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Account Management Policy **State:** DIR Security Control Standards Catalog **Federal:** NIST SP 800-162, 800-178, 800-192; FBI CJIS CSP v5.9	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures for addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; system-generated list of temporary accounts removed and/or disabled; system-generated list of emergency accounts removed and/or disabled; system audit records; system security plan; other relevant documents or record.

Interview: Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities; system developers

Test: Automated mechanisms for implementing account management functions.

AC-02(04): AUTOMATED AUDIT ACTIONS

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

Automatically audit account creation, modification, enabling, disabling, and removal actions.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - Account management information sources include systems, appliances, devices, services, and applications (including databases). Automated account management audit action results must be delivered in a format compliant with DFPS requirements. Results must be unaltered, searchable, and made available to DFPS Office of Information Security.

Std.02 - DFPS Information Technology Services (ITS) disables all accounts that have not been accessed for 30 days. ITS archives employee accounts that have not been accessed for 90 days

SUPPLEMENTAL GUIDANCE

Account management audit records are defined in accordance with AU-02 and reviewed, analyzed, and reported in accordance with AU-06.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Account Management Policy **State:** DIR Security Control Standards Catalog **Federal:** NIST SP 800-162, 800-178, 800-192; FBI CJIS CSP v5.9	AU-2, AU-6.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing account management; system design documentation; system configuration settings and associated documentation; notifications/alerts of account creation, modification, enabling, disabling, and removal actions; system audit records; system security plan; other relevant documents or records.

Interview: Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities.

Test: Automated mechanisms implementing account management functions

AC-02(05): INACTIVITY LOGOUT

Priority: P1

Baseline(s): Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

Require that users log out when unattended except as defined in the access control policy.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - Require that users log out when unattended except as defined in the access control policy.

SUPPLEMENTAL GUIDANCE

Inactivity logout is behavior or policy-based and requires users to take physical action to log out when they are expecting inactivity longer than the defined period. Automatic enforcement of inactivity logout is addressed by AC-11.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Account Management Policy **State:** DIR Security Control Standards Catalog **Federal:** NIST SP 800-162, 800-178, 800-192.	AU-11

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing account management; system design documentation; system configuration settings and associated documentation; security violation reports; system audit records; system security plan; other relevant documents or records.

Interview: Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities; users that must comply with inactivity logout policy.

AC-02(07): ROLE-BASED SCHEMES

Priority: P1

Baseline(s): Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

a. Establish and administer privileged user accounts in accordance with [Selection: a role-based access scheme; an attribute-based access scheme];

b. Monitor privileged role or attribute assignments;

c. Monitor changes to roles or attributes; and

d. Revoke access when privileged role or attribute assignments are no longer appropriate.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - All privileged roles accounts are separate administrative accounts that are authorized to perform system and security related functions that ordinary users are not authorized to perform. To minimize access to these controls, each IT administrator must use a separate account for day-to-day activities that doesn't have administrative privileges.

SUPPLEMENTAL GUIDANCE

Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. These privileged roles include, for example, key management, account management, network and system administration, database administration, and web administration.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP 800-162, 800-178, 800-192; FBI CJIS CSP v5.9	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing account management; system design documentation; system configuration settings and associated documentation; system-generated list of privileged user accounts and associated roles; records of actions taken when privileged role assignments are no longer appropriate; system audit records; audit tracking and monitoring reports; system monitoring records; system security plan; other relevant documents or records.

Interview: Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities.

Test: Automated mechanisms implementing account management functions; automated mechanisms monitoring privileged role assignments.

AC-02(12): ACCOUNT MONITORING / ATYPICAL USAGE

Priority: P1

Baseline(s): Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

a. Monitor system accounts for atypical usage; and

b. Report atypical usage of system accounts to defined personnel or roles (defined in the applicable system security plan), and if necessary, incident response team.

AGENCY IMPLEMENTATION STANDARDS

Std.01 – The DFPS Office of Information Security uses automated tools to monitor atypical system account usage. Atypical usage includes accessing systems at certain times of the day or from locations that are not consistent with the normal usage patterns of individuals. Monitoring for atypical usage may reveal rogue behavior by individuals or an attack in progress

The agency utilizes anomaly detection software for user and entity behavioral analytics (UEBA) and machine learning (ML). Risk is evaluated by looking different risk indicators, grouped into risk factors, as follows:

SUPPLEMENTAL GUIDANCE

Atypical usage includes, for example, accessing information systems at certain times of the day and from locations that are not consistent with the normal usage patterns of individuals working in organizations.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP 800-162, 800-178, 800-192.	AU-6, AU-7, CA-7, IR-8, SI-4.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control for atypical usage for which to monitor system accounts is defined; personnel or roles to report atypical usage is/are defined; system accounts are monitored for atypical usage; Atypical usage of system accounts is reported to defined personnel or roles.

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing account management; system design documentation; system configuration settings and associated documentation; system monitoring records; system audit records; audit tracking and monitoring reports; privacy impact assessment; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities

Test: Automated mechanisms implementing account management functions.

AC-02(13): DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

a. The organization disables accounts of users posing a significant risk immediately, not to exceed 30 minutes for High risk systems or 60 minutes for Moderate systems after discovery of the risk.

AGENCY IMPLEMENTATION STANDARDS

Std.01 – Disable accounts immediately upon report of any indication of compromise as defined in the System Security Plan (see SI-04).

Std.02 - Re-enable accounts with additional protections as appropriate only after incident handling process is complete.

Std.03 - Automated system account management includes using automated mechanisms to disable user accounts flagged as high-risk due to atypical usage outlined in AC-02(12).

SUPPLEMENTAL GUIDANCE

Users posing a significant risk to organizations include individuals for whom reliable evidence or intelligence indicates either the intention to use authorized access to information systems to cause harm or through whom adversaries will cause harm. Harm includes potential adverse impacts to organizational operations and assets, individuals, other organizations, or the Nation. Close coordination between authorizing officials, information system administrators, and human resource managers is essential in order for timely execution of this control enhancement.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP 800-162, 800-178, 800-192.	AU-6, SI-4.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control including a time period within which to disable accounts of individuals who are discovered to pose significant risk is defined; significant risks leading to disabling accounts are defined; accounts of individuals are disabled within defined time period of discovery of significant risks.

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing account management; system design documentation; system configuration settings and associated documentation; system-generated list of disabled accounts; list of user activities posing significant organizational risk; system audit records; system security plan; other relevant documents or records.

Interview: Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities

Test: Automated mechanisms implementing account management functions.

AC-03: ACCESS ENFORCEMENT

Priority: P1	
Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - Access to state information resources shall be appropriately managed. [Source: DIR Control Standards Catalog AC-3]

Std.02 - Each user of information resources shall be assigned a unique identifier except for situations where risk analysis demonstrates no need for individual accountability of users.

Std.03 - User identification shall be authenticated before the information resources system may grant that user access. [Source: DIR Control Standards Catalog AC-3]

Std.04 - Restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.

Std.05 - If encryption is used as an access control mechanism it must meet DFPS approved (FIPS 140-2 compliant) encryption standards (see SC-13).

SUPPLEMENTAL GUIDANCE

Access control policies control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (i.e., devices, files, records, domains) in organizational systems. In addition to enforcing authorized access at the system level and recognizing that systems can host many applications and services in support of mission and business functions, access enforcement mechanisms can also be employed at the application and service level to provide increased information security and privacy. In contrast to logical access controls that are implemented within the system, physical access controls are addressed by the controls in the Physical and Environmental Protection (PE) family.

Security-relevant information is any information within the system that can potentially impact the operation of security functions in a manner that could result in failure to enforce the system security policy or maintain isolation of code and data. Secure, non-operable system states are states in which the system is not performing mission/business-related processing (for example, the system is offline for maintenance, troubleshooting, bootup, and shutdown).

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** OMB A-130; NIST SP 800-57-1, 800-57-2, 800-57-3, 800-162, 800-178; NIST IR 7874; Privacy Act; FBI CJIS CSP v5.9 Section	AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AC-24, AC-25, AT-2, AT-3, AU-9, CA-9, CM-5, CM-11, IA-2, IA-5, IA-6, IA-7, IA-11, MA-3, MA-4, MA-5, MP-4, PM-2, PS-3, PT-2, PT-3, SA-17, SC-2, SC-3, SC-4, SC-12, SC-13, SC-28, SC-31, SC-34, SI-4, SI-8.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control including approved authorizations for logical access to information and system resources are enforced in accordance with applicable access control policies.

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing access enforcement; system design documentation; system configuration settings and associated documentation; list of approved authorizations (user privileges); system audit records; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with access enforcement responsibilities; system/network administrators; organizational personnel with information security and privacy responsibilities; system developers.

Test: Automated mechanisms implementing access control policy.

AC-3(03): MANDATORY ACCESS CONTROL

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The information system enforces organization-defined mandatory access control policy over all subjects and objects where the policy:

a. Is uniformly enforced across all subjects and objects within the boundary of the information system;
b. Specifies that a subject that has been granted access to information is constrained from doing any of the following;
1. Passing the information to unauthorized subjects or objects;
2. Granting its privileges to other subjects;
3. Changing one or more security attributes on subjects, objects, the information system, or information system component
4. Choosing the security attributes and attribute values to be associated with newly created or modified objects; or
5. Changing the rules governing access control; and
6. Specifies that organization-defined subjects may explicitly be granted organization-defined privileges (i.e., they are trusted subjects) such that they are not limited by some or all of the above constraints.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - Any DFPS information system with CJI must enforce assigned authorizations for controlling access to the system and contained information. The information system controls must restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.

Std.02 - Explicitly authorized personnel include, for example, application security administrators, system and network administrators, cybersecurity administrators and other privileged users with access to system control, monitoring, or administration functions (e.g. information system security officers, maintainers, system programmers).

Std.03 - Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) must be employed by DFPS to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system.

SUPPLEMENTAL GUIDANCE

Mandatory access control as defined in this control enhancement is synonymous with nondiscretionary access control and is not constrained only to certain historical uses (e.g., implementations using the Bell-LaPadula Model). The above class of mandatory access control policies constrains what actions subjects can take with information obtained from data objects for which they have already been granted access, thus preventing the subjects from passing the information to unauthorized subjects and objects. This class of mandatory access control policies also constrains what actions subjects can take with respect to the propagation of access control privileges; that is, a subject with a privilege cannot pass that privilege to other subjects. The policy is uniformly enforced over all subjects and objects to which the information system has control. Otherwise, the access control policy can be circumvented. This enforcement typically is provided via an implementation that meets the reference monitor concept (see AC-25). The policy is bounded by the information system boundary (i.e., once the information is passed outside of the control of the system, additional means may be required to ensure that the constraints on the information remain in effect). The trusted subjects described above are granted privileges consistent with the concept of least privilege (see AC-6). Trusted subjects are only given the minimum privileges relative to the above policy necessary for satisfying organizational mission/business needs. The control is most applicable when there is some policy mandate (e.g., law, Executive Order, directive, or regulation) that establishes a policy regarding access to sensitive/classified information and some users of the information system are not authorized access to all sensitive/classified information resident in the information system. This control can operate in conjunction with AC-3(4). A subject that is constrained in its operation by policies governed by this control is still able to operate under the less rigorous constraints of AC-3(4), but policies governed by this control take precedence over the less rigorous constraints of AC-3(4). For example, while a mandatory access control policy imposes a constraint preventing a subject from passing information to another subject operating at a different sensitivity label, AC-3(4) permits the subject to pass the information to any subject with the same sensitivity label as the subject.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** FBI CJIS CSP v5.9	SC-7.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; mandatory access control policies; procedures addressing access enforcement; system design documentation; system configuration settings and associated documentation; list of subjects and objects (i.e., users and resources) requiring enforcement of mandatory access control policies; system audit records; system security plan; other relevant documents or records

Interview: Organizational personnel with access enforcement responsibilities; system/network administrators; organizational personnel with information security responsibilities; system developers.

Test: Automated mechanisms implementing mandatory access control.

AC-3(04): DISCRETIONARY ACCESS CONTROL

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The information system enforces organization-defined discretionary access control policy over defined subjects and objects where the policy specifies that a subject that has been granted access to information can do one or more of the following:

a. Pass the information to any other subjects or objects;
b. Grant its privileges to other subjects;
c. Change security attributes on subjects, objects, the information system, or the information system's components;
d. Choose the security attributes to be associated with newly created or revised objects; or
e. Change the rules governing access control.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - Any DFPS information system with CJI must enforce assigned authorizations for controlling access to the system and contained information. The information system controls must restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.

Std.02 - Explicitly authorized personnel include, for example, application security administrators, system and network administrators, cybersecurity administrators and other privileged users with access to system control, monitoring, or administration functions (e.g. information system security officers, maintainers, system programmers).

Std.03 - Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) must be employed by DFPS to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system.

SUPPLEMENTAL GUIDANCE

When discretionary access control policies are implemented, subjects are not constrained with regard to what actions they can take with information for which they have already been granted access. Thus, subjects that have been granted access to information are not prevented from passing (i.e., the subjects have the discretion to pass) the information to other subjects or objects. This control enhancement can operate in conjunction with AC-3(3). A subject that is constrained in its operation by policies governed by AC-3(3) is still able to operate under the less rigorous constraints of this control enhancement. Thus, while AC-3(3) imposes constraints preventing a subject from passing information to another subject operating at a different sensitivity level, AC-3(4) permits the subject to pass the information to any subject at the same sensitivity level. The policy is bounded by the information system boundary. Once the information is passed outside of the control of the information system, additional means may be required to ensure that the constraints remain in effect. While the older, more traditional definitions of discretionary access control require identity-based access control, that limitation is not required for this use of discretionary access control.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **Federal:** FBI CJIS CSP v5.9	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; discretionary access control policies; procedures addressing access enforcement; system design documentation; system configuration settings and associated documentation; list of subjects and

objects (i.e., users and resources) requiring enforcement of discretionary access control policies; system audit records; system security plan; other relevant documents or records.

Interview: Organizational personnel with access enforcement responsibilities; system/network administrators; organizational personnel with information security responsibilities; system developers.

Test: Automated mechanisms implementing discretionary access control policy.

AC-04: INFORMATION FLOW ENFORCEMENT

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on information flow control policies as defined in System Security Plans (SSPs), Information Security Architecture, and Information Security Agreements (ISAs).

AGENCY IMPLEMENTATION STANDARDS

Std.01 - Ensure that only the required information, and not more, is communicated.

Std.02 - Agency-issued unique identifiers are administered from a centralized access control system to ensure that levels of authorization between interconnected systems are consistently applied for each authorized user.

Information control enforcement measures may also include, but are not limited to, the following:

1. Access control lists (ACL);
2. Documented business justifications for the use of all services, protocols, and ports allowed;
3. Explicit security attributes on information, source, and destination objects;
4. Demilitarized zones (DMZ) implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports;
5. Anti-spoofing measures implemented if feasible to detect and block forged source IP addresses from entering the network;
6. Implementing stateful inspection (dynamic packet filtering);
7. Placing system components that store PII within in internal network zone, segregated from the DMZ and any untrusted networks; and
8. Prohibiting private IP addresses and routing information from being disclosed to unauthorized parties.

SUPPLEMENTAL GUIDANCE

Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include, for example, keeping export-controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, restricting web requests to the Internet that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content. Transferring information between information systems representing different security domains with different security pol8icies introduces risk that such transfers violate one or more domain security policies. In such situations, information owners/stewards provide guidance at designated policy enforcement points between interconnected systems. Organizations consider mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes, for example: (i) prohibiting information transfers between interconnected systems (i.e., allowing access only); (ii) employing hardware mechanisms to enforce one-way information flows; and (iii) implementing trustworthy regrading mechanisms to reassign security attributes and security labels.

Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations (e.g., networks, individuals, and devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices (e.g., gateways, routers, guards, encrypted tunnels, firewalls) that employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or

message-filtering capability based on message content (e.g., implementing key word searches or using document characteristics). Organizations also consider the trustworthiness of filtering/inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement. Control enhancements 3 through 22 primarily address cross-domain solution needs which focus on more advanced filtering techniques, in-depth analysis, and stronger flow enforcement mechanisms implemented in cross-domain products, for example, high-assurance guards. Such capabilities are generally not available in commercial off-the-shelf information technology products.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP-800-160-1, 800-162, 800-178; NIST IR 8112; FBI CJIS CSP v5.9	AC-3, AC-6, AC-16, AC-17, AC-19, AC-21, AU-10, CA-3, CA-9, CM-7, PL-9, PM-24, SA-17, SC-4, SC-7, SC-16, SC-31.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has information flow control policies within the system and between connected systems are defined; approved authorizations are enforced for controlling the flow of information within the system and between connected systems based on information flow control policies;

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; information flow control policies; procedures addressing information flow enforcement; security architecture documentation; privacy architecture documentation; system design documentation; system configuration settings and associated documentation; system baseline configuration; list of information flow authorizations; system audit records; system security plan; privacy plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security and privacy architecture development responsibilities; organizational personnel with information security and privacy responsibilities; system developers.

Test: Automated mechanisms implementing information flow enforcement policy.

AC-4(08): SECURITY POLICY FILTERS

Priority: P1

Baseline(s): High	Overlay(s): N/A

CONTROL REQUIREMENTS

The information system enforces information flow control using best available security policy filters, or like technology to filter on selected PII values as a basis for flow control decisions for prevention of unauthorized transfer of PII across information system boundaries or domains.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - Information system enforces information flow control using best available security policy filters to filter on selected sensitive information values as a basis for flow control decisions for prevention of unauthorized transfer of selected sensitive information across information system boundaries or domains.

Std.02 - Block or Quarantine data after a filter processing failure in accordance with the DFPS Data Loss Prevention Policy.

SUPPLEMENTAL GUIDANCE

Security policy filters, or like technology, such as data loss prevention (DLP), can provide a form of continuous monitoring for compliance with privacy laws and regulations. Implementation of this security control reduces the potential for unauthorized transfer of PII, CJIS or other sensitive data types.

Organization-defined security policy filters can address data structures and content. For example, security policy filters for data structures can check for maximum file lengths, maximum field sizes, and data/file types (for structured and unstructured data). Security policy filters for data content can check for specific words (e.g., dirty/clean word filters), enumerated values or data value ranges, and hidden content. Structured data permits the interpretation of data content by applications. Unstructured data typically refers to digital information without a particular data structure or with a data structure that does not facilitate the development of rule sets to address the particular sensitivity of the information conveyed by the data or the associated flow enforcement decisions. Unstructured data consists of: (i) bitmap objects that are inherently non-language-based (i.e., image, video, or audio files); and (ii) textual objects that are based on written or printed languages (e.g., commercial off-the-shelf word processing documents, spreadsheets, or emails). Organizations can implement more than one security policy filter to meet information flow control objectives (e.g., employing clean word lists in conjunction with dirty word lists may help to reduce false positives).

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Data Loss Prevention Policy.	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented security policy filters to be used as a basis for enforcing information flow control are defined; privacy policy filters to be used as a basis for enforcing information flow control are defined; information flows for which information flow control is enforced by security filters are defined; one or more of the following parameters is/are selected: block; strip; modify; quarantine.

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; information flow control policies; procedures addressing information flow enforcement; system design documentation; system configuration settings and associated documentation; list of security policy filters regulating flow control decisions; list of privacy policy filters regulating flow control decisions; system audit records; system security plan; privacy plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security and privacy responsibilities; system developers

Test: Automated mechanisms implementing information flow enforcement policy; security and privacy policy filter.

AC-05: SEPARATION OF DUTIES

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

a. Identify and document duties of user types in the System Security Plan (SSP) to prevent malicious activity without collusion; and

b. Define system access authorizations to support separation of duties

AGENCY IMPLEMENTATION STANDARDS

Std.01 – Ensure adequate controls and separation of duties for tasks that are susceptible to fraudulent or other unauthorized activity. [Source: DIR Control Standards Catalog AC-5]

Std.02 - It is recommended to separate administration/operation, management/allocations, and audit/testing functions, and separate responsibilities for critical system functions among different individuals.

Examples of functions and sub-functions that should be considered for assignment to different individuals include:

1. Data Creation and Control Functions:
   a. Data collection and preparation;
   b. Data entry;
   c. Data verification, reconciliation of output and approval; and
   d. Database administration.
2. Software Development and Maintenance Functions:
   a. Applications programming;
   b. Design Review;
   c. Application testing and evaluation; and
   d. Application Maintenance.
3. Security Functions
   a. Security implementation; and
   b. Review of security controls, security audits, and audit trail review.

NOTE: Input of transactions that may result in a conflict of interest, fraud, abuse, or direct financial loss (for example, input of vendor invoices and purchasing and receiving information) shall be separated.

SUPPLEMENTAL GUIDANCE

Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes dividing mission or business functions and support functions among different individuals or roles, conducting system support functions with different individuals, and ensuring that security personnel who administer access control functions do not also administer audit functions. Because separation of duty violations can span systems and application domains, organizations consider the entirety of systems and system components when developing policy on separation of duties. Separation of duties is enforced through the account management activities in AC-02, access control mechanisms in AC-03, and identity management activities in IA-02, IA-04, and IA-12.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** FBI CJIS CSP v5.9	AC-2, AC-3, AC-6, AU-9, CM-5, CM-11, CP-9, IA-2, IA-4, IA-5, IA-12, MA-3, MA-5, PS-2, SA-8, SA-17.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing divisions of responsibility and separation of duties; system configuration settings and associated documentation; list of divisions of responsibility and separation of duties; system access authorizations; system audit records; system security plan; other relevant documents or records.

Interview: Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties; organizational personnel with information security responsibilities; system/network administrators.

Test: Automated mechanisms implementing separation of duties policy.

AC-06: LEAST PRIVILEGE

Priority: P1

Baseline(s):Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

AGENCY IMPLEMENTATION STANDARDS

Std.01 – Limit access to system components and cardholder data to only those individuals whose job requires such access.

a. Define access needs for each role, including:
   1. System components and data resources that each role needs to access for their job function; and
   2. Level of privilege required (for example, user, administrator, etc.) for accessing resources.
b. Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.
c. Assign access based on individual personnel's job classification and function.
d. Require documented approval by authorized parties specifying required privileges.

SUPPLEMENTAL GUIDANCE

Organizations employ least privilege for specific duties and systems. The principle of least privilege is also applied to system processes, ensuring that the processes have access to systems and operate at privilege levels no higher than necessary to accomplish organizational missions or business functions. Organizations consider the creation of additional processes, roles, and accounts as necessary to achieve least privilege.

Organizations apply least privilege to the development, implementation, and operation of organizational systems.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** FBI CJIS CSP v5.9	AC-2, AC-3, AC-6, AU-9, CM-5, CM-11, CP-9, IA-2, IA-4, IA-5, IA-12, MA-3, MA-5, PS-2, SA-8, SA-17.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing divisions of responsibility and separation of duties; system configuration settings and associated documentation; list of divisions of responsibility and separation of duties; system access authorizations; system audit records; system security plan; other relevant documents or records.

Interview: Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties; organizational personnel with information security responsibilities; system/network administrators.

Test: Automated mechanisms implementing separation of duties policy.

AC-06(01): AUTHORIZE ACCESS TO SECURITY FUNCTIONS

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

At a minimum, the organization explicitly authorizes access to the following list of security functions (deployed in hardware, software, and firmware) and security-relevant information:

a. Setting/modifying audit logs and auditing behavior;

b. Setting/modifying boundary protection system rules;

c. Configuring/modifying access authorizations (i.e., permissions, privileges);

d. Setting/modifying authentication parameters; and

e. Setting/modifying system configurations and parameters

AGENCY IMPLEMENTATION STANDARDS

Std.01 - Authorize access for personnel or roles as defined in System Security Plans (SSPs) to:

a. Security functions (deployed in hardware, software, and firmware) as defined in SSPs; and

b. Security-relevant information as defined in Std.02.

Std.02 - At a minimum, explicitly authorize access (based on role) to the following list of security functions and security-relevant information:

a. Setting/modifying audit logs and auditing behavior;

b. Setting/modifying boundary protection system rules;

c. Configuring/modifying access authorizations (i.e., permissions, privileges);

d. Setting/modifying authentication parameters; and

e. Setting/modifying system configurations and parameters

SUPPLEMENTAL GUIDANCE

Security functions include establishing system accounts, configuring access authorizations (i.e., permissions, privileges), configuring settings for events to be audited, and establishing intrusion detection parameters. Security-relevant information includes filtering rules for routers or firewalls, configuration parameters for security services, cryptographic key management information, and access control lists. Authorized personnel include security administrators, system administrators, system security officers, system programmers, and other privileged users.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** FBI CJIS CSP v5.9	AC-17, AC-18, AC-19, AU-9, PE-2.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing least privilege; list of security functions (deployed in hardware, software, and firmware) and security-relevant information for which access must be explicitly authorized; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

Interview: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks; organizational personnel with information security responsibilities; system/network administrators.

Test: Automated mechanisms implementing least privilege functions

AC-06(02): NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

Require that users of system accounts (or roles) with access to any security functions or security-relevant information use non-privileged accounts or roles, when accessing non-security functions.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - DFPS requires that users of information system accounts with access to security functions or security-relevant information use administrative accounts for accessing security related information and use non-privileged accounts when accessing non-security functions. This control enhancement limits exposure when operating from within privileged accounts or roles.

SUPPLEMENTAL GUIDANCE

Requiring the use of non-privileged accounts when accessing non-security functions limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies, such as role- based access control, and where a change of role provides the same degree of assurance in the change of access authorizations for the user and the processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account.

REFERENCES	RELATED CONTROLS

Agency: DFPS Information Security Policy. **State:** TX Govt. Code 552; DIR Security Control Standards Catalog. **Federal:** FBI CJIS CSP v5.9	AC-17, AC-18, AC-19, PL-4.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing least privilege; list of system-generated security functions or security-relevant information assigned to system accounts or roles; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records

Interview: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks; organizational personnel with information security responsibilities; system/network administrators.

Test: Automated mechanisms implementing least privilege functions.

AC-06(05): PRIVILEGED ACCOUNTS

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization restricts privileged accounts on the information system to personnel with roles requiring privileged access and defined in the system security plan.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - DFPS requires privileged accounts for administrative functions and uses a separate non-privileged account to perform internet browsing, email functions, word processing, etc.

Std.02 - Restrict privileged accounts to the minimum number required. Limit super-user/root privileges to the maximum extent possible.

SUPPLEMENTAL GUIDANCE

Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from accessing privileged information or privileged functions. Organizations may differentiate in the application of restricting privileged accounts between allowed privileges for local accounts and for domain accounts provided that they retain the ability to control system configurations for key parameters and as otherwise necessary to sufficiently mitigate risk.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** TX Govt. Code 552; DIR Security Control Standards Catalog. **Federal:** FBI CJIS CSP v5.9	IA-2, MA-3, MA-4.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing least privilege; list of system-generated security functions or security-relevant information assigned to system accounts or roles; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records

Interview: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks; organizational personnel with information security responsibilities; system/network administrators.

Test: Automated mechanisms implementing least privilege functions.

AC-06(07): REVIEW OF USER PRIVILEGES

Priority: P1

Baseline(s): Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization:

a. Review at least annually the privileges assigned to roles or classes of users as defined in the System Security Plan (SSP) to validate the need for such privileges; and

b. Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - The administrator who is assigned the responsibility for overseeing user accounts, or that person's designee, reviews all accounts and permissions at least annually. This review makes sure each user has appropriate access and privileges related to the user's job title and functions. Accounts are also reviewed if DFPS Information Technology Services (ITS) or Office of Information Security (OIS) has reason to believe access and privileges are not appropriate for users' job functions.

SUPPLEMENTAL GUIDANCE

The need for certain assigned user privileges may change over time to reflect changes in organizational mission and business functions, environments of operation, technologies, or threats. A periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Account Management Policy. **State:** DIR Security Control Standards Catalog.	CA-7.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing least privilege; list of system-generated security functions or security-relevant information assigned to system accounts or roles; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records

Interview: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks; organizational personnel with information security responsibilities; system/network administrators.

Test: Automated mechanisms implementing least privilege functions.

AC-06(09): LOG USE OF PRIVILEGED FUNCTIONS

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The information system audits the execution of privileged functions.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - Ensure that applications produce audit records containing sufficient information to identify the actor, time of action, type of action, and which component, feature, or function of the application was accessed as defined in the System Security Plan (SSP).

SUPPLEMENTAL GUIDANCE

Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the Advanced Persistent Threat (APT).

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** TX Govt. Code 552; Bus. & Comm. 521; DIR Security Control Standards Catalog. **Federal:** FBI CJIS CSP v5.9	AU-2, AU-3, AU-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing least privilege; list of system-generated security functions or security-relevant information assigned to system accounts or roles; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

Interview: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks; organizational personnel with information security responsibilities; system/network administrators.

Test: Automated mechanisms implementing least privilege functions.

AC-06(10): PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - Limit system access to the types of transactions and functions that authorized users are permitted to execute, either by specific account or by account type.

SUPPLEMENTAL GUIDANCE

Privileged functions include disabling, circumventing, or altering implemented security or privacy controls, establishing system accounts, performing system integrity checks, and administering cryptographic key management activities. Non-privileged users are individuals who do not possess appropriate authorizations. Privileged functions that require protection from non-privileged users include circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms. Preventing non-privileged users from executing privileged functions is enforced by AC-03.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** TX Govt. Code 552; Bus. & Comm. 521; DIR Security Control Standards Catalog.	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing least privilege; system design documentation; system configuration settings and associated documentation; list of privileged functions and associated user account assignments; system audit records; system security plan; other relevant documents or records.

Interview: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks; organizational personnel with information security responsibilities; system developers.

Test: Automated mechanisms implementing least privilege functions for non-privileged users

AC-07: UNSUCCESSFUL LOGON ATTEMPTS

Priority: P1

Baseline(s):Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The information system:

a. Enforce a limit of, as identified in the DFPS Information Security Policy (Locking Accounts after Unsuccessful Access Attempts), a number of consecutive invalid logon attempts by a user during a period as defined in the DFPS Information Security Policy; and
b. Automatically disables or locks the account/node until released by an administrator or after the time period specified in DFPS Information Security Policy when the maximum number of unsuccessful attempts is exceeded.

AGENCY IMPLEMENTATION STANDARDS

Std. 01 – As technology permits, enforce account lockouts after no more than 5 failed attempts. This threshold may be lowered for Moderate or High-risk systems. Require the lockout to persist for a minimum of 15 minutes unless released by an administrator. [Source: DIR Control Standards Catalog AC-7]

NOTE: Users may contact the DFPS Customer Service Center (DFPS IT Help Desk) to release the user account prior to the lockout's expiration if the lockout hinders productivity.

Std.02 - For cloud service providers, providers configure the information system to:

a. Enforce a limit of not more than five (5) consecutive invalid login attempts by a user during a 15-minute time period; and
b. Automatically lock the account/node for 30 minutes when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection.

SUPPLEMENTAL GUIDANCE

Organizations employ least privilege for specific duties and systems. The principle of least privilege is also applied to system processes, ensuring that the processes have access to systems and operate at privilege levels no higher than necessary to accomplish organizational missions or business functions. Organizations consider the creation of additional processes, roles, and accounts as necessary to achieve least privilege.

Organizations apply least privilege to the development, implementation, and operation of organizational systems.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** TX Govt. Code 552; DIR Security Control Standards Catalog. **Federal:** NIST SP 800-63-3, 800-124; FBI CJIS CSP v5.9	AC-2, AC-9, AU-2, AU-6, IA-5.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing unsuccessful logon attempts; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records

Interview: Organizational personnel with information security responsibilities; system developers; system/network administrators.

Test: Automated mechanisms implementing access control policy for unsuccessful logon attempts.

AC-08: SYSTEM USE NOTIFICATION

Priority: P1

Baseline(s):Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The information system:

a) Display the official DFPS System Use Notification to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:

1. Users are accessing a DFPS system;
2. System usage may be monitored, recorded, and subject to audit;
3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
4. Use of the system indicates consent to monitoring and recording;

b) Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and

c) For publicly accessible systems:

1. Display system use information unless and until the user takes positive action (for example, clicking a button indicating "OK") to acknowledge agreement, before granting further access to the publicly accessible system;
2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
3. Include a description of the authorized uses of the system.

AGENCY IMPLEMENTATION STANDARDS

Std. 01 – System Identification/Logon Banner. System identification/logon banners shall have warning statements that include the following topics:

a. Unauthorized use is prohibited;
b. Usage may be subject to security testing and monitoring;
c. Misuse is subject to criminal prosecution; and
d. Users have no expectation of privacy except as otherwise provided by applicable privacy laws.

[Source: DIR Control Standards Catalog AC-8].

The mandated system notification message (warning banner) for all Agency-owned information resources must read as shown below:

WARNING: This is a Department of Family and Protective (DFPS) computer system, which should be accessed and used only for approved DFPS business by authorized personnel. Unauthorized access or use of this computer

system may subject violators to disciplinary action, up to and including termination of employment as well as criminal prosecution.

All information on this computer system may be intercepted, recorded, and disclosed, by and to, authorized personnel for security testing and other official purposes including criminal investigations. Access or use of this computer system by any person whether authorized or unauthorized constitutes consent to these items.

USING THIS SYSTEM CARRIES WITH IT NO EXPECTATION OF PRIVACY!!!

SUPPLEMENTAL GUIDANCE

System use notifications can be implemented using messages or warning banners displayed before individuals log in to information systems. System use notifications are used only for access via logon interfaces with human users and are not required when such human interfaces do not exist. Organizations consider system use notification messages/banners displayed in multiple languages based on specific organizational needs and the demographics of information system users. Organizations also consult with the Office of the General Counsel for legal review and approval of warning banner content.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** FBI CJIS CSP v5.9	AC-14, PL-4, SI-4.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; privacy and security policies, procedures addressing system use notification; documented approval of system use notification messages or banners; system audit records; user acknowledgements of notification message or banner; system design documentation; system configuration settings and associated documentation; system use notification messages; system security plan; privacy plan; privacy impact assessment; privacy assessment report; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security and privacy responsibilities; legal counsel; system developers.

Test: Automated mechanisms implementing system use notification.

AC-11: SESSION LOCK

Priority: P1

Baseline(s):Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The information system:

1. Prevents further access to the system by initiating a session lock after fifteen (15) minutes of inactivity (for both remote and internal access connections) or upon receiving a request from a user; and
2. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

AGENCY IMPLEMENTATION STANDARDS

Std. 01 – All DFPS-owned information resources must implement a session lock that takes effect after 15 minutes of inactivity.

SUPPLEMENTAL GUIDANCE

Device locks are temporary actions taken to prevent logical access to organizational systems when users stop work and move away from the immediate vicinity of those systems but do not want to log out because of the temporary nature of their absences. Device locks can be implemented at the operating system level or at the application level. A proximity lock may be used to initiate the device lock (e.g., via a Bluetooth-enabled device or dongle). User-initiated device locking is behavior or policy-based and, as such, requires users to take physical action to initiate the device lock. Device locks are not an acceptable substitute for logging out of systems, such as when organizations require users to log out at the end of workdays.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** FBI CJIS CSP v5.9	AC-14, PL-4, SI-4.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing session lock; procedures addressing identification and authentication; system design documentation; system configuration settings and associated documentation; security plan; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; system developers.

Test: Automated mechanisms implementing access control policy for session lock.

AC-11(01): PATTERN-HIDING DISPLAYS

Priority: P1

Baseline(s):Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.

AGENCY IMPLEMENTATION STANDARDS

Std. 01 – Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity. [Source: SP 800-171 3.1.10]

Std.02 - The pattern-hiding display can include a static image, such as solid colors, clock, battery life indicator with the caveat that sensitive information is not displayed.

SUPPLEMENTAL GUIDANCE

Publicly viewable images can include static or dynamic images, for example, patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen, with the additional caveat that none of the images conveys sensitive information.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** TX Govt. Code 2054.516; DIR Security Control Standards Catalog. **Federal:** FBI CJIS CSP v5.9	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing session lock; display screen with session lock activated; system design documentation; system configuration settings and associated documentation; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; system developers.

Test: System session lock mechanisms.

AC-12: SESSION TERMINATION

Priority: P1

Baseline(s):Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The information system automatically terminates a user session after the user logs out of the system or removes the token (authenticator), or after thirty (30) minutes of inactivity.

AGENCY IMPLEMENTATION STANDARDS

Std. 01 – For moderate and high-baseline systems, configure applications to terminate user sessions and require user re-authentication in accordance with the DFPS Identification and Authentication Standard.

Std.02 - For web and mobile applications, avoid non-expiring session cookies and set a reasonable expiration time for idle sessions. This will help protect user sessions from misuse if the cookie is captured.

Std.03 - For Web and mobile applications, configure applications to terminate user sessions and require user re-authentication.

Std.03 - For Web and mobile applications, new sessions should be generated each time a user is authenticated.

Std.04 - For Web and mobile applications, sessions should be destroyed when a user logs out.

SUPPLEMENTAL GUIDANCE

Session termination addresses the termination of user-initiated logical sessions (in contrast to SC-10, which addresses the termination of network connections associated with communications sessions (i.e., network disconnect)). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational system. Such user sessions can be terminated without terminating network sessions. Session termination ends all processes associated with a user's logical session except for those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events that require automatic termination of the session include organization-defined periods of user inactivity, targeted responses to certain types of incidents, or time-of-day restrictions on system use.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** TX Govt. Code 2054.516; DIR Security Control Standards Catalog.	MA-4, SC-10, SC-23.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing session termination; system design documentation; system configuration settings and associated documentation; list of conditions or trigger events requiring session disconnect; system audit records; system security plan; other relevant documents or records

Interview: System/network administrators; organizational personnel with information security responsibilities; system developers.

Test: Automated mechanisms implementing user session termination.

AC-12(01): USER-INITIATED LOGOUTS / MESSAGE DISPLAYS

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The information system:

(a) Provides a logout capability for user-initiated communications sessions whenever authentication is used to gain access to CJIS information resources; and

(b) Displays an explicit logout message to users indicating the reliable termination of authenticated communications sessions.

AGENCY IMPLEMENTATION STANDARDS

Std. 01 – Any DFPS information system with CJI must enforce assigned authorizations for controlling access to the system and contained information. The information system controls must restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.

Explicitly authorized personnel include, for example, application security administrators, system and network administrators, cybersecurity administrators and other privileged users with access to system control, monitoring, or administration functions (e.g. information system security officers, maintainers, system programmers).

Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) must be employed by DFPS IT to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system.

External vendors obtaining CJI through DFPS must adhere to the same controls.

SUPPLEMENTAL GUIDANCE

Information resources to which users gain access via authentication include, for example, local workstations, databases, and password-protected websites/web-based services. Logout messages for web page access, for example, can be displayed after authenticated sessions have been terminated. However, for some types of interactive sessions including, for example, file transfer protocol (FTP) sessions, information systems typically send logout messages as final messages prior to terminating sessions.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FBI CJIS CSP v5.9	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing session termination; system design documentation; system configuration settings and associated documentation; list of conditions or trigger events requiring session disconnect; system audit records; system security plan; other relevant documents or records

Interview: System/network administrators; organizational personnel with information security responsibilities; system developers.

Test: Automated mechanisms implementing user session termination.

AC-14: PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization:

a. Identifies specific user actions that can be performed on the information system without identification or authentication consistent with organizational mission and business functions;

b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

AGENCY IMPLEMENTATION STANDARDS

Std. 01 – Identify, document, and provide supporting rationale in the security plan for any actions that may be performed on an information system without identification or authentication. [Source: DIR Control Standards Catalog AC-14]

Std.02 - Define stipulations in the System Security Plan (SSP) for bypassing identification and authentication mechanisms to facilitate operations in emergency situations

SUPPLEMENTAL GUIDANCE

Specific user actions may be permitted without identification or authentication if organizations determine that identification and authentication are not required for the specified user actions. Organizations may allow a limited number of user actions without identification or authentication, including when individuals access public websites or other publicly accessible federal systems, when individuals use mobile phones to receive calls, or when facsimiles are received. Organizations identify actions that normally require identification or authentication but may, under certain circumstances, allow identification or authentication mechanisms to be bypassed. Such bypasses may occur, for example, via a software-readable physical switch that commands bypass of the logon functionality and is protected from accidental or unmonitored use. Permitting actions without identification or authentication does not apply to situations where identification and authentication have already occurred and are not repeated but rather to situations where identification and authentication have not yet occurred. Organizations may decide that there are no user actions that can be performed on organizational systems without identification and authentication, and therefore, the value for the assignment operation can be "none."

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog.	AC-8, IA-2, PL-2.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing permitted actions without identification or authentication; system configuration settings and associated documentation; security plan; list of user actions that can be performed without identification or authentication; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities.

AC-17: REMOTE ACCESS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

If remote access is authorized, the organization:

a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and

b. Authorizes remote access to the information system prior to allowing such connections.

AGENCY IMPLEMENTATION STANDARDS

Std. 01 – DFPS must establish, document, and review usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed. [Source: DIR Control Standards Catalog AC-17]

Std.02 - All remote access connections must be authorized prior to allowing such connections. [Source: DIR Control Standards Catalog AC-17]

Std.03 — Configurations Requirement:

a) Direct access to DFPS network is only provided when using VPN while working remotely.

b) All remote access to the network must use an organization approved encrypted connection in compliance with SC-13.

c) Multi-factor authentication is required for all remote access.

Std.04 — Usage Restrictions:

a) Use only organization authorized and approved devices for remote access to organization non-public systems;

b) Take every reasonable effort to ensure the confidentiality, integrity, and availability of information and information systems used remotely (for example, not leaving laptops and other devices unattended or in public plain view); and

c) Users must understand their responsibilities for protecting Sensitive, Confidential, or Controlled data and the consequences for mishandling such data.

d) The DFPS CISO must authorize the execution of privileged commands and access to security-relevant information, like logging into a firewall device for administrative functions. Remote access under these conditions must be executed by authorized personnel only for compelling operational needs. Such actions must be logged and audited.

Std.05 — Implementation Guidance:

a) Approved devices remotely connecting to the organization network must have a VPN client installed, with an organization issued VPN certificate;

b) Implement adequate security measures (e.g., virus, malware, and spam protection, firewall, intrusion detection) on client computers prior to allowing VPN remote access;

c) Virtual desk application shall be securely configured to minimize the ability of users to copy data;

d) The information system shall use automated functions to monitor and control remote access methods;

e) Systems must log all remote access occurrences, including both end user and administrator activity user credential, date/time, and duration of connection at a minimum); and

f) Route all remote accesses through managed network access control points. Limiting the number of access control points for remote accesses reduces the attack surface for organizations.

g) No public access to RDP or SSH shall be permitted; all connections must either initiate within the Agency's protected network or via a secure gateway. RDP and SSH shall be configured to enforce TLS connections.

SUPPLEMENTAL GUIDANCE

Remote access is access to organizational information systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet). Remote access methods include, for example, dial-up, broadband, and wireless. Organizations often employ encrypted virtual private networks (VPNs) to enhance confidentiality and integrity over remote connections. The use of encrypted VPNs does not make the access non-remote; however, the use of VPNs, when adequately provisioned with appropriate security controls (e.g., employing appropriate encryption techniques for confidentiality and integrity protection) may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks. Still, VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote connections. Also, VPNs with encrypted tunnels can affect the organizational capability to adequately monitor network communications traffic for malicious code. Remote access controls apply to information systems other than public web servers or systems designed for public access. This control addresses authorization prior to allowing remote access without specifying the formats for such authorization. While organizations may use interconnection security agreements to authorize remote access connections, such agreements are not required by this control. Enforcing access restrictions for remote connections is addressed in AC-3.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FBI CJIS CSP v5.9	AC-2, AC-3, AC-4, AC-18, AC-19, AC-20, CA-3, CM-10, IA-2, IA-3, IA-8, MA-4, PE-17, PL-2, PL-4, SC-10, SC-12, SC-13, SI-4.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing remote access to the system; system design documentation; system configuration settings and associated documentation; system audit records; system monitoring records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; system developers.

Test: Automated mechanisms monitoring and controlling remote access methods.

AC-17(01): AUTOMATED MONITORING / CONTROL

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The information system monitors and controls remote access methods.

AGENCY IMPLEMENTATION STANDARDS

Std. 01 – All remote access connections should employ automated mechanisms to monitor and control remote access methods when technically feasible.

SUPPLEMENTAL GUIDANCE

Automated monitoring and control of remote access sessions allows organizations to detect cyber-attacks and also ensure ongoing compliance with remote access policies by auditing connection activities of remote users on a variety of information system components (e.g., servers, workstations, notebook computers, smart phones, and tablets).

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: NIST SP 800-46, 800-77, 800-113, 800-114, 800-121; NIST IR 7966; FBI CJIS CSP v5.9	AU-2, AU-6, AU-12, AU-14.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing remote access to the system; system design documentation; system configuration settings and associated documentation; system audit records; system monitoring records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; system developers.

Test: Automated mechanisms monitoring and controlling remote access methods.

AC-17(02): PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The information system routes all remote accesses through a limited number of managed access control points.

AGENCY IMPLEMENTATION STANDARDS

Std. 01 – Encryption for all remote access sessions over networks outside DFPS authorization boundaries must comply with SC-13.

SUPPLEMENTAL GUIDANCE

Virtual private networks can be used to protect the confidentiality and integrity of remote access sessions. Transport Layer Security (TLS) is an example of a cryptographic protocol that provides end-to-end communications security over networks and is used for Internet communications and online transactions.

REFERENCES	RELATED CONTROLS

Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: NIST SP 800-46, 800-77, 800-113, 800-114, 800-121; NIST IR 7966; FBI CJIS CSP v5.9	SC-8, SC-12, SC-13.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing remote access to the system; system design documentation; system configuration settings and associated documentation; cryptographic mechanisms and associated configuration documentation; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; system developers.

Test: Cryptographic mechanisms protecting confidentiality and integrity of remote access sessions.

AC-17(03): MANAGED ACCESS CONTROL POINTS

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The information system routes remote accesses through authorized and managed network access control points.

AGENCY IMPLEMENTATION STANDARDS

Std. 01 – DFPS information systems must route all remote accesses through a limited number of managed access control points.

SUPPLEMENTAL GUIDANCE

Organizations consider the Trusted Internet Connections (TIC) initiative requirements for external network connections since limiting the number of access control points for remote access reduces attack surfaces.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: NIST SP 800-46, 800-77, 800-113, 800-114, 800-121; NIST IR 7966; FBI CJIS CSP v5.9	SC-7.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing remote access to the system; system design documentation; list of all managed network access control points; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities.

Test: Automated mechanisms routing all remote accesses through managed network access control points.

AC-17(04): PRIVILEGED COMMANDS / ACCESS

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization:

a. Authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs; and

b. Documents the rationale for such access in the security plan for the information system.

AGENCY IMPLEMENTATION STANDARDS

Std. 01 – DFPS must document and define the authorization of executing of privileged commands and access to security-relevant information via remote access with the rationale for such access in System Security Plans (SSPs).

SUPPLEMENTAL GUIDANCE

Remote access to systems represents a significant potential vulnerability that can be exploited by adversaries. As such, restricting the execution of privileged commands and access to security-relevant information via remote access reduces the exposure of the organization and the susceptibility to threats by adversaries to the remote access capability.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: NIST SP 800-46, 800-77, 800-113, 800-114, 800-121; NIST IR 7966; FBI CJIS CSP v5.9	AC-6, SC-12, SC-13.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS
Examine: Access control policy; procedures addressing remote access to the system; system configuration settings and associated documentation; security plan; system audit records; system security plan; other relevant documents or records. Interview: System/network administrators; organizational personnel with information security responsibilities. Test: Automated mechanisms implementing remote access management.

AC-17(06): PROTECTION OF INFORMATION

Priority: P1	
Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS
The organization ensures that users protect information about remote access mechanisms from unauthorized use and disclosure.

AGENCY IMPLEMENTATION STANDARDS
Std. 01 – DFPS must ensures that users protect information about remote access mechanisms from unauthorized use and disclosure.

SUPPLEMENTAL GUIDANCE
Remote access to systems represents a significant potential vulnerability that can be exploited by adversaries. As such, users must ensure that users protect information about remote access mechanisms from unauthorized use and disclosure.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: NIST SP 800-46, 800-77, 800-113, 800-114, 800-121; NIST IR 7966; FBI CJIS CSP v5.9	AT-2, AT-3, PS-6.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS
Examine: Access control policy; procedures addressing remote access to the system; system security plan; other relevant documents or records. Interview: Organizational personnel with responsibilities for implementing or monitoring remote access to the system; system users with knowledge of information about remote access mechanisms; organizational personnel with information security responsibilities.

AC-17(09) DISCONNECT OR DISABLE ACCESS

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

Provide the capability to disconnect or disable remote access to the system within the periods defined in Stds.02 & 03.

AGENCY IMPLEMENTATION STANDARDS

Std. 01 –Terminate or suspend network connections (that is, system-to-system interconnections) upon issuance of an order by the DFPS CIO, CISO, or Legal Counsel.

Std.02 — High baseline systems must have the capability to be disconnected within 10 minutes.

Std.03 — Moderate baseline systems must have the capability to be disconnected within 20 minutes.

SUPPLEMENTAL GUIDANCE

The speed of system disconnects or disablement varies based on the criticality of missions or business functions and the need to eliminate immediate or future remote access to systems.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: NIST SP 800-46, 800-77, 800-113, 800-114, 800-121; NIST IR 7966.	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing disconnecting or disabling remote access to the system; system design documentation; system configuration settings and associated documentation; security plan, system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; system developers.

Test: Automated mechanisms implementing capability to disconnect or disable remote access to system.

AC-18: WIRELESS ACCESS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

If wireless access is authorized, the organization:

a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for each type of wireless access; and

b. Authorizes each type of wireless access to the information system prior to allowing such connections.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Establish the requirements and security restrictions for installing or providing access to information resources systems. The wireless policy shall address the following topic areas:

a. Wireless Local Area Networks. Ensure that Service Set Identifiers (SSID) values are changed from the manufacturer default setting. Some networks should not include organizational or location information in the SSID. Additional equipment configuration recommendations are included in the Wireless Security Guidelines.

b. Types of information that may be transmitted via wireless networks and devices with or without encryption including mission critical information or sensitive personal information. DFPS must not transmit confidential information via a wireless connection to, or from a portable computing device unless encryption methods, such as a Virtual Private Network (VPN), Wi-Fi Protected Access, or other secure encryption protocols that meet appropriate protection or certification standards, are used to protect the information.

c. Prohibit and periodically monitor any unauthorized installation or use of Wireless Personal Area Networks on state organizational IT systems by individuals without the approval of the information resources manager. [Source: DIR Control Standards Catalog AC-18]

Std.02 — For wireless environments connected to the DFPS data environment, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.

Std.03 — Implement processes to test for the presence of wireless access points (802.11) and detect and identify all authorized and unauthorized wireless access points on an annual basis at a minimum.

Std.04 - Confidential information must not be transmitted via wireless connection to, or from, a mobile computing device unless encryption methods that appropriately secure wireless transmissions, such as Virtual Private Network (VPN), Wi-Fi Protected Access (WPA-2) or other secure encryption protocols are utilized.

SUPPLEMENTAL GUIDANCE

Wireless technologies include microwave, packet radio (ultra-high frequency or very high frequency), 802.11x, and Bluetooth. Wireless networks use authentication protocols that provide authenticator protection and mutual authentication.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: NIST SP 800-94, 800-97; FBI CJIS CSP v5.9	AC-2, AC-3, AC-17, AC-19, CA-9, CM-7, IA-2, IA-3, IA-8, PL-4, SC-40, SC-43, SI-4.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing wireless access implementation and usage (including restrictions); configuration management plan; system design documentation; system configuration settings and associated documentation; wireless access authorizations; system audit records; system security plan; other relevant documents or records.

Interview: Organizational personnel with responsibilities for managing wireless access connections; organizational personnel with information security responsibilities.

Test: Wireless access management capability for the system.

AC-18(01): AUTHENTICATION AND ENCRYPTION

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

Protect wireless access to the system using authentication of both users and devices as appropriate (for example, devices to wireless networks and users to enterprise services) and encryption.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Implement Extensible Authentication Protocol (EAP) with Wi-Fi Access Protection or IEEE 802.11i on WLANs or access points to provide encryption and strong identification and authentication for moderate- and high-impact systems.

Std.02 — Verify that wireless communications are mutually authenticated. [Source: OWASP: Application Security Verification Standard C.9]

SUPPLEMENTAL GUIDANCE

Wireless networking capabilities represent a significant potential vulnerability that can be exploited by adversaries. To protect systems with wireless access points, strong authentication of users and devices along with strong encryption can reduce susceptibility to threats by adversaries involving wireless technologies.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: NIST SP 800-94, 800-97; FBI CJIS CSP v5.9	SC-8, SC-12, SC-13.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing wireless implementation and usage (including restrictions); system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; system developers.

Test: Automated mechanisms implementing wireless access protections to the system.

AC-18(03): DISABLE WIRELESS NETWORKING

Priority: P1

Baseline(s): Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - Wireless networking capabilities embedded within system components must be disabled prior to issuance and deployment when not intended for use or wireless network capabilities are not approved by the DFPS CISO.

SUPPLEMENTAL GUIDANCE

Wireless networking capabilities that are embedded within system components represent a significant potential vulnerability that can be exploited by adversaries. Disabling wireless capabilities when not needed for essential organizational missions or functions can reduce susceptibility to threats by adversaries involving wireless technologies.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** Bus. & Comm. 521; DIR Security Control Standards Catalog. **Federal**: NIST SP 800-94, 800-97; FBI CJIS CSP v5.9	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing wireless implementation and usage (including restrictions); system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; system developers.

Test: Automated mechanisms managing the disabling of wireless networking capabilities internally embedded within system components.

AC-18(05): ANTENNAS / TRANSMISSION POWER LEVELS

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization selects radio antennas and calibrates transmission power levels to reduce the probability that usable signals can be received outside of organization-controlled boundaries.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — The Texas Department of Public Safety (DPS) is responsible for selecting the satellite and radio antennas that transmit CJI to DFPS to reduce the probability that usable signals can be received outside of organization-controlled boundaries.

Std.02 — No outside equipment such as coffeepots, TV's, radios, etc., should use any electrical outlets that are assigned for the TLETS satellite/radio use since it could cause interference on the connection or equipment.

SUPPLEMENTAL GUIDANCE

Actions that may be taken by organizations to limit unauthorized use of wireless communications outside of organization-controlled boundaries include, for example: (i) reducing the power of wireless transmissions so that the transmissions are less likely to emit a signal that can be used by adversaries outside of the physical perimeters of organizations; (ii) employing measures such as TEMPEST to control wireless emanations; and (iii) using directional/beam forming antennas that reduce the likelihood that unintended receivers will be able to intercept signals. Prior to taking such actions, organizations can conduct periodic wireless surveys to understand the radio frequency profile of organizational information systems as well as other systems that may be operating in the area.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: NIST SP 800-94, 800-97; FBI CJIS CSP v5.9	PE-19.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing wireless implementation and usage (including restrictions); system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities.

Test: Calibration of transmission power levels for wireless access; radio antenna signals for wireless access; wireless access reception outside of organization-controlled boundaries.

AC-19: ACCESS CONTROL FOR MOBILE DEVICES

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and

b. Authorize the connection of mobile devices to organizational systems.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS must establish usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, whether owned by DFPS or the employee. [Source: DIR Control Standards Catalog AC-19]

Std.02 — Encrypt information on all mobile devices that contains DFPS Confidential and Controlled Information with an appropriate encryption technique that meets Federal Information Processing Standard 140-2 in accordance with SC-13.

Std.03 — Agency-owned mobile devices are joined to the Agency's mobile device management (MDM) system and may access any Agency information resource at the same level of authorization given to an Agency workstation.

Std.04 - Any mobile device that connects to an Agency information resource must install and comply with the Agency’s MDM tool and App Protection Policies (APP), like container encryption, to ensure devices are updated with current release operating system software approved by the vendor and meet security baseline requirements.

Std.05 - All mobile devices that access Agency information resources must utilize a passcode to prevent unauthorized access to the mobile device and a PIN or biometrics to access Agency managed applications.

Std.06 - All remote access to confidential information from a portable computing device must utilize encryption techniques, such as Virtual Private Network (VPN), Secure File Transfer Protocol (SFTP), or Secure Sockets Layers (SSL).

Std.07 - Mobile computing devices that access Agency information resources must be encrypted, patched/updated, and protected with anti-virus software. Any mobile computing device that is personally owned cannot contain Confidential information; and if it contains Controlled information it must be encrypted, patched/updated, and protected with anti-virus software.

Std.08 - All devices (personal and Agency owned) compliance is monitored by the Agency’s MDM tool and Mobile Application Management (MAM) policies. Devices out of compliance with security baselines and policies will not be allowed to access Agency resources.

SUPPLEMENTAL GUIDANCE

A mobile device is a computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the device to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, E-readers, and tablets. Mobile devices are typically associated with a single individual and the device is usually in close proximity to the individual; however, the degree of proximity can vary depending upon on the form factor and size of the device. The processing, storage, and transmission capability of the mobile device may be comparable to or merely a subset of desktop systems, depending upon the nature and intended purpose of the device. Due to the large variety of mobile devices with different technical characteristics and capabilities, organizational restrictions may vary for the different classes/types of such devices. Usage restrictions and specific implementation guidance for mobile devices include, for example, configuration management, device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Organizations are cautioned that the need to provide adequate security for mobile devices goes beyond the requirements in this control. Many safeguards and countermeasures for mobile devices are reflected in other security controls in the catalog allocated in the initial control baselines as starting points for the development of security plans and overlays using the tailoring process. There may also be some degree of overlap in the requirements articulated by the security controls within the different families of controls. AC-20 addresses mobile devices that are not organization-controlled.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: NIST SP 800-114, 800-124; FBI CJIS CSP v5.9	AC-3, AC-4, AC-7, AC-11, AC-17, AC-18, AC-20, CA-9, CM-2, CM-6, IA-2, IA-3, MP-2, MP-4, MP-5, MP-7, PL-4, SC-7, SC-34, SC-43, SI-3, SI-4.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing access control for mobile device usage (including restrictions); configuration management plan; system design documentation; system configuration settings and associated documentation; authorizations for mobile device connections to organizational systems; system audit records; system security plan; other relevant documents or records.

Interview: Organizational personnel using mobile devices to access organizational systems; system/network administrators; organizational personnel with information security responsibilities.

Test: Access control capability for mobile device connections to organizational systems; configurations of mobile devices.

AC-19(05): FULL DEVICE / CONTAINER-BASED ENCRYPTION

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization employ full-device encryption where possible, and container-based encryption otherwise to protect the confidentiality and integrity of information on all mobile devices authorized to connect to DFPS information systems.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — For mobile devices containing Personally Identifiable Information (PII) and Criminal Justice Information (CJI), employ encryption to protect the confidentiality and integrity of information on mobile devices (e.g., smartphones and laptop computers) in accordance with SC-13.

Std.02 — All mobile devices (including, but not limited to, smartphones, tablets, diagnostics, and calibration devices) must employ DFPS-defined mobile device management and encryption solutions in accordance with AC-19.

Std.03 — All DFPS mobile devices must use enterprise solutions for file-based encryption, full-disk, or full-device encryption.

SUPPLEMENTAL GUIDANCE

Container-based encryption provides a more fine-grained approach to the encryption of data/information on mobile devices, including for example, encrypting selected data structures such as files, records, or fields.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FBI CJIS CSP v5.9	SC-12, SC-13, SC-28.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing access control for mobile devices; system design documentation; system configuration settings and associated documentation; encryption mechanisms and associated configuration documentation; system audit records; system security plan; other relevant documents or records.

Interview: Organizational personnel with access control responsibilities for mobile devices; system/network administrators; organizational personnel with information security responsibilities.

Test: Encryption mechanisms protecting confidentiality and integrity of information on mobile devices.

AC-20: USE OF EXTERNAL INFORMATION SYSTEMS

Priority: P1	
Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:
1. Access the system from external systems; and
2. Process, store, or transmit organization-controlled information using external systems; or

b. Prohibit the use of all types of external systems except as authorized per Stds.03 & 04.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Develop policies governing the use of external information systems and resources including the type and classification of data that can be stored outside of DFPS. [Source: DIR Control Standards Catalog AC-20]

Std.02 — Establish terms and conditions for contracting with external information resources providers. [Source: DIR Control Standards Catalog AC-20]

Std.03 — Limit connections to and use of external systems to only those required for business operations.

Std.04 — Establish and document terms and conditions via Interconnection Security Agreements (ISAs).

Std.05 — The DFPS chief information officer must approve all external information resources prior to their use within the Agency. Information owners must individually conduct a risk assessment for any information under their control before allowing the use of an external information resource to process, store, or transmit such information.

Std.06 — The use of an external information resource for the processing, storage, or transmission of mission-critical or confidential information must be approved in advance by the DFPS chief information security officer.

Std.07 - The DFPS Office of Information Security will maintain a list of currently approved external information resources.

SUPPLEMENTAL GUIDANCE

External systems are systems that are used by but not part of organizational systems, and for which the organization has no direct control over the implementation of required controls or the assessment of control effectiveness. External systems include personally owned systems, components, or devices; privately owned computing and communications devices in commercial or public facilities; systems owned or controlled by nonfederal organizations; systems managed by contractors; and federal information systems that are not owned by, operated by, or under the direct supervision or authority of the organization. External systems also include systems owned or operated by other components within the same organization and systems within the organization with different authorization boundaries.

Organizations have the option to prohibit the use of any type of external system or prohibit the use of specified types of external systems, (e.g., prohibit the use of any external system that is not organizationally owned or prohibit the use of personally-owned systems).

For some external systems (i.e., systems operated by other organizations), the trust relationships that have been established between those organizations and the originating organization may be such that no explicit terms and conditions are required. Systems within these organizations may not be considered external. These situations occur when, for example, there are pre-existing information exchange agreements (either implicit or explicit) established between organizations or components or when such agreements are specified by applicable laws, executive orders, directives, regulations, policies, or standards.

Authorized individuals include organizational personnel, contractors, or other individuals with authorized access to organizational systems and over which organizations have the authority to impose specific rules of behavior regarding system access. Restrictions that organizations impose on authorized individuals need not be uniform, as the restrictions may vary depending on trust relationships between organizations. Therefore, organizations may choose to impose different security restrictions on contractors than on state, local, or tribal governments.

External systems used to access public interfaces to organizational systems are outside the scope of AC-20. Organizations establish specific terms and conditions for the use of external systems in accordance with organizational security policies and procedures. At a minimum, terms and conditions address the specific types of applications that can be accessed on organizational systems from external systems and the highest security category of information that can be processed, stored, or transmitted on external systems. If the terms and

conditions with the owners of the external systems cannot be established, organizations may impose restrictions on organizational personnel using those external systems.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FIPS 199; NIST SP 800-171, 800-172; FBI CJIS CSP v5.9	AC-2, AC-3, AC-17, AC-19, CA-3, PL-2, PL-4, SA-9, SC-7.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing the use of external systems; external systems terms and conditions; list of types of applications accessible from external systems; maximum security categorization for information processed, stored, or transmitted on external systems; system configuration settings and associated documentation; system security plan; other relevant documents or records.

Interview: Organizational personnel with responsibilities for defining terms and conditions for use of external systems to access organizational systems; system/network administrators; organizational personnel with information security responsibilities.

Test: Automated mechanisms implementing terms and conditions on use of external systems.

AC-20(01): LIMITS ON AUTHORIZED USE

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization:

a. Permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after:

1. Verification of the implementation of controls on the external system as specified in the organization's security and privacy policies and security and privacy plans; or
2. Retention of approved system connection or processing agreements with the organizational entity hosting the external system.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — The DFPS CISO must approve all external information resources prior to their use within the Agency. Information owners must inform the Office of Information Security of proposed external connections and conduct a risk assessment for any information under their control before allowing the use of an external information resource to process, store, or transmit such information.

SUPPLEMENTAL GUIDANCE

Limiting authorized use recognizes circumstances where individuals using external systems may need to access organizational systems. Organizations need assurance that the external systems contain the necessary controls so as not to compromise, damage, or otherwise harm organizational systems. Verification that the required controls have been implemented can be achieved by external, independent assessments, attestations, or other means, depending on the confidence level required by organizations.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FIPS 199; NIST SP 800-171, 800-172; FBI CJIS CSP v5.9	CA-2.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing the use of external systems; system connection or processing agreements; account management documents; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities.

Test: Automated mechanisms implementing limits on use of external systems.

AC-20(02): PORTABLE STORAGE DEVICES

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization:

a. Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems using the restrictions defined in Stds.01 & 02.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — All portable storage devices connecting to DFPS systems must comply with the DFPS Information Security Policy - Removable Media procedures.

Std.02 — Rewritable devices must be scanned for malware prior to accessing DFPS systems after any use on non-DFPS systems.

Std.02 — DFPS-owned portable storage devices may be used on external systems but data cannot be transferred from those devices to the external systems without explicit approval from the DFPS CISO. Other file transfer processes are preferred, like electronic mail or SFTP.

SUPPLEMENTAL GUIDANCE

Limits on the use of organization-controlled portable storage devices in external systems include restrictions on how the devices may be used and under what conditions the devices may be used.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FIPS 199; NIST SP 800-171, 800-172; FBI CJIS CSP v5.9	MP-7, SC-41.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing the use of external systems; system configuration settings and associated documentation; system connection or processing agreements; account management documents; system security plan; other relevant documents or records.

Interview: Organizational personnel with responsibilities for restricting or prohibiting the use of organization-controlled storage devices on external systems; system/network administrators; organizational personnel with information security responsibilities.

Test: Automated mechanisms implementing restrictions on use of portable storage devices.

AC-21: INFORMATION SHARING

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for information sharing circumstances as described in the Information Sharing Agreement (ISA), where user discretion is required; and

b. Employ automated or manual review processes as described in Std.01 to assist users in making information sharing and collaboration decisions.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Access authorizations must be documented in the System Security Plan (SSP) and reviewed at least as often as the SSP for currency, business need, and to ensure that no intentional or unintentional information sharing with unauthorized parties occurs.

Std.02 — Provide training to authorized users on the mechanisms or processes available for making appropriate sharing decisions, specifically including access restrictions for data classifications.

Std.03 — DFPS Information owners which permit sharing of information under their control are responsible for ensuring all authorized users understand the information owner's sharing policy, and for reviewing levels of access, to include sharing to external partners, at least every 12 months.

Std.04 — The Texas Department of Information Resources (DIR) shall establish an information sharing and analysis organization to provide a forum for state agencies, local governments, public and private institutions of higher education, and the private sector to share information regarding cybersecurity threats, best practices, and remediation strategies.

a. DIR shall provide administrative support to the information sharing and analysis organization.
b. A participant in the information sharing and analysis organization shall assert any exception available under state or federal law, including Section 552.139, in response to a request for public disclosure of information shared through the organization. Section 552.007 does not apply to information described by this subsection. [Source: TX Govt. Code 2054.0594]

SUPPLEMENTAL GUIDANCE

Information sharing applies to information that may be restricted in some manner based on some formal or administrative determination. Examples of such information include, contract-sensitive information, classified information related to special access programs or compartments, privileged information, proprietary information, and personally identifiable information. Security and privacy risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to these determinations. Depending on the circumstances, sharing partners may be defined at the individual, group, or organizational level. Information may be defined by content, type, security category, or special access program or compartment. Access restrictions may include non-disclosure agreements (NDA). Information flow techniques and security attributes may be used to provide automated assistance to users making sharing and collaboration decisions.

Sharing information can help to manage risks. This information may include vulnerabilities, threats, security incidents and mitigation measures, criticality of systems and components, or delivery information for supply chain risk management. This information sharing should be carefully managed to ensure that the information is accessible only to authorized individuals with a legitimate business need.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** TX Govt. Code 2054; DIR Security Control Standards Catalog. **Federal**: OMB A-130; NIST SP 800-150; NIST IR 8062; FBI CJIS CSP v5.9	AC-3, AC-4, AC-16, PT-2, PT-7, RA-3, SC-15.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing user-based collaboration and information sharing (including restrictions); system design documentation; system configuration settings and associated documentation; system-generated list of users authorized to make information-sharing/collaboration decisions; system-generated list of sharing partners and access authorizations; system-generated list of access restrictions regarding information to be shared; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; system developers.

Test: Automated mechanisms implementing access authorizations supporting information-sharing/user collaboration decisions.

AC-22: PUBLICLY ACCESSIBLE CONTENT

Priority: P1	
Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Designate individuals authorized to make information publicly accessible;
b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and
d. Review the content on the publicly accessible system for nonpublic information quarterly or as new information is posted and remove such information, if discovered.
e. users in making information sharing and collaboration decisions.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Develop policies governing the procedures to post information on publicly accessible information systems. [Source: DIR Control Standards Catalog AC-22]

Std.02 — If Sensitive, Confidential, or Controlled information is discovered on a public site, the information must be handled according to the organization's incident management policies and procedures.

SUPPLEMENTAL GUIDANCE

Posting information on non-organizational systems (e.g., non-organizational public websites, forums, and social media) is covered by organizational policy. While organizations may have individuals who are responsible for developing and implementing policies about the information that can be made publicly accessible, publicly accessible content addresses the management of the individuals who make such information publicly accessible.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: Privacy Act; FBI CJIS CSP v5.9	AC-3, AT-2, AT-3, AU-13.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing publicly accessible content; list of users authorized to post publicly accessible content on organizational systems; training materials and/or records; records of publicly accessible information reviews; records of response to non-public information on public websites; system audit logs; security awareness training records; system security plan; other relevant documents or records.

Interview: Organizational personnel with responsibilities for managing publicly accessible information posted on organizational systems; organizational personnel with information security responsibilities.

Test: Automated mechanisms implementing management of publicly accessible content.

AC-23: DATA MINING PROTECTION

Priority: P1

Baseline(s): N/A	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization employs methods for email or data files containing criminal justice information (CJI) to adequately detect and protect against data mining.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — The metadata derived from CJI must not be used by any cloud service provider for any purposes. The cloud service provider is prohibited from scanning any email or data files for the purpose of building analytics, data mining, advertising, or improving the services provided.

SUPPLEMENTAL GUIDANCE

Data mining is an analytical process that attempts to find correlations or patterns in large data sets for the purpose of data or knowledge discovery. Data storage objects include database records and database fields. Sensitive information can be extracted from data mining operations. When information is personally identifiable information, it may lead to unanticipated revelations about individuals and give rise to privacy risks. Prior to performing data mining activities, organizations determine whether such activities are authorized. Organizations may be subject to applicable laws, executive orders, directives, regulations, or policies that address data mining requirements. Organizational personnel consult with the senior agency official for privacy and legal counsel regarding such requirements.

Data mining prevention and detection techniques include limiting the number and frequency of database queries to increase the work factor needed to determine the contents of databases, limiting types of responses provided to database queries, applying differential privacy techniques or homomorphic encryption, and notifying personnel when atypical database queries or accesses occur. Data mining protection focuses on protecting information from data mining while such information resides in organizational data stores. In contrast, AU-13 focuses on monitoring for organizational information that may have been mined or otherwise obtained from data stores and is available as open-source information residing on external sites, such as social networking or social media websites.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **Federal**: FBI CJIS CSP v5.9	PM-12, PT-2.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures for preventing and detecting data mining; policies and procedures addressing authorized data mining techniques; procedures addressing protection of data storage objects against data mining; system design documentation; system configuration settings and associated documentation; system audit logs; system audit records; procedures addressing differential privacy techniques; notifications of atypical database queries or accesses; documentation or reports of insider threat program; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with responsibilities for implementing data mining detection and prevention techniques for data storage objects; legal counsel; organizational personnel with information security and privacy responsibilities; system developers.

Test: Automated mechanisms implementing data mining prevention and detection.

(AT) AWARENESS AND TRAINING

The DFPS organization requires that users of DFPS information systems are made aware of the security risks associated with their activities and of the applicable laws, policies, standards, or procedures related to the security of DFPS information systems. The DFPS organization requires that DFPS personnel are complying with Agency security awareness training requirements.

The control sets in the AT Control Family are specific to security training and procedures, including security training records. The intended audience for this Control includes, but is not limited to, all users of DFPS information systems (including contractors), information resource owners and custodians.

AT-01: SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Develops, documents, and disseminates to personnel/roles as designated by the organization:
   1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and

b. Reviews and, if necessary, updates the current:
   1. Security awareness and training policy at least once every three (2) years (or if there is significant change);and
   2. Security awareness and training procedures at least once every three hundred sixty-five (365) days.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — The DFPS Commissioner or his/her designated representative(s) shall ensure that the agency has trained personnel to assist the agency in complying with the requirements of 1 TAC 202 and related policies. [Source: 1 TAC 202.20(4)]

Std.02 — Establish the requirements to ensure each user of information resources receives adequate training on computer security issues. [Source: DIR Control Standards Catalog AT-1]

Std.03 — The DFPS Chief Information Security Officer shall be responsible for:

a. Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks;
b. Providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities under 1 TAC 202; and

c. Developing and recommending policies and establishing procedures and practices, in cooperation with the agency Information Resources Manager, information-owners and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, or disclosure. [Source: 1 TAC 202.21(b)(3, 5, 8)]

Std.04 — All users of DFPS-owned information resources must undergo information security awareness training approved by the DFPS Chief Information Security Officer or their designee at a schedule established by DFPS Office of Information Security.

Std.05 — DFPS personnel who use information resources are required to comply with the policy and procedures related to Security Awareness and must acknowledge they have read, understand, and will comply with agency requirements regarding computer security policies and procedures through the DFPS Acceptable Use Agreement (AUA) .

Std.06 — The DFPS Office of Information Security will prescribe any additional required training for users with access to confidential, sensitive, or mission-critical information resources, and users with privileged access to information resources.

SUPPLEMENTAL GUIDANCE

Awareness and training policy and procedures address the controls in the AT family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of awareness and training policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations.

Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to awareness and training policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Acceptable Use Agreement; DFPS Phishing Security Awareness Training. **State:** 1 TAC 202.20(4), DIR Security Control Standards Catalog **Federal**: NIST SP 800-12, 800-30, 800-39, 800-50, 800-100; CJIS CSP v5.9 Section 5.2.1	PM-9, PS-8, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System security plan; privacy plan; awareness and training policy and procedures; other relevant documents or records.

Interview: Organizational personnel with awareness and training responsibilities; organizational personnel with information security and privacy responsibilities.

AT-02: SECURITY AWARENESS TRAINING

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors):

1. As part of initial training for new users and annually thereafter; and

2. When required by system changes or following major changes to legislation or security requirements;

b. Employ the following techniques to increase the security and privacy awareness of system users: awareness techniques in accordance with the awareness and training policy, procedures, and standards;

c. Update literacy training and awareness content annually and following major changes to legislation or security requirements; and

d. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS Office of Information Security shall:

a. Provide an ongoing information security awareness education program for all users; and

b. Use new employee orientation to introduce information security awareness and inform new employees of information security policies and procedures. [Source: DIR Control Standards Catalog AT-2]

c. All users must acknowledge they have read, understand, and will comply with the agency requirements regarding computer security policies and procedures through the DFPS Acceptable Use Agreement (AUA).

d. All DFPS employees must complete security awareness training on an annual basis.

e. DFPS Office of Information Security may require additional incidental training and require acknowledgement as determined by the department.

f. Between training cycles, the DFPS Office of Information Security shall employ other communications channels (such as email, Agency intranet, digital signage, and awareness campaigns such as National Cyber Security Awareness Month) to inform users of information security awareness topics.

Std.02 — An agency-wide information security program must be approved by the DFPS Commissioner and include administering an ongoing information security awareness education program for all users; and introducing information security awareness and informing new employees of information security policies and procedures during the onboarding process. [Source: 1 TAC 202.24(b)(2, 3)]

Std.03 — The DFPS Commissioner or their designee shall verify completion of a cybersecurity training program by employees of the state agency in a manner specified by DIR. Additionally, the DFPS Commissioner or their designee shall periodically require an internal review of the agency to ensure compliance with TX Govt. Code 2054.5191. [Source: TX Govt. Code 2054.5191(c, d)]

Std.04 — DFPS may select the most appropriate cybersecurity training program certified under TX Govt Code 2054.519 for employees of the state agency. [Source: TX Govt. Code 2054.519 (c)]

Std.05 — DFPS requires any contractor who has access to a state computer system or database to complete a cybersecurity training program certified under TX Govt. Code 2054.519 as selected by the agency. The cybersecurity training program must be completed by a contractor during the term of the contract and during any renewal period. A contractor required to complete a cybersecurity training program under this section shall verify completion of the program to the contracting state agency. [Source: TX Govt. Code 2054.5192(b, c, e)]

Std.06 — Required completion of a cybersecurity training program must be included in the terms of a contract awarded by DFPS to a contractor. [Source: TX Govt. Code 2054.5192(d)]

Std.07 — The person(s) who oversees contract management for DFPS shall report the contractor's completion to the department; and periodically review agency contracts to ensure compliance with this section. [Source: TX Govt. Code 2054.5192(e)]

Std.08 — All users with authorized access to CJI must be aware of their individual responsibilities and expected behavior when accessing CJI and the systems which process CJI. External agencies are required to administer CJIS training approved by the Department of Public Safety (DPS) or the Federal Bureau of Investigations (FBI) that meet requirement or process required by federal, state, or local laws.

Std.08 — CJIS security awareness training will be required within six months of hire, and biennially thereafter, for all personnel who have access to CJI to include all personnel who have unescorted access to a physically secure location.

SUPPLEMENTAL GUIDANCE

Organizations determine the appropriate content of security and privacy awareness training, and security and privacy awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and privacy, and to respond to suspected security and privacy incidents. The content also addresses awareness of the need for operations security and privacy as it relates to DFPS's information security program. Security and privacy awareness techniques can include, for example, displaying posters, offering supplies inscribed with security and privacy reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security and privacy awareness events.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Acceptable Use Agreement; DFPS Phishing Security Awareness Training; DFPS Contractor Data and System Security Requirements. **State:** 1 TAC 202.24(b)(2, 3); TX Govt. Code 2054.135(d), TX Govt. Code 2054.519, TX Govt. Code 2054.5191, TX Govt. Code 2054.5192; DIR Security Control Standards Catalog **Federal**: NIST SP 800-12, 800-30, 800-39, 800-50, 800-100; CJIS CSP v5.9 Section 5.2.1	AC-3, AC-17, AC-22, AT-3, AT-4, CP-3, IA-4, IR-2, IR-7, IR-9, PL-4, PM-13, PM-21, PS-7, PT-2, SA-8, SA-16.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System security plan; privacy plan; literacy training and awareness policy; procedures addressing literacy training and awareness implementation; appropriate codes of federal regulations; security and privacy literacy training curriculum; security and privacy literacy training materials; training records; other relevant documents or records.

Interview: Organizational personnel with responsibilities for literacy training and awareness; organizational personnel with information security and privacy responsibilities; organizational personnel comprising the general system user community.

Test: Automated mechanisms managing information security and privacy literacy training.

AT-02(01): PRACTICAL EXERSIZES

Priority: P1	
Baseline(s): Low, Moderate, High	Overlay(s): N/A
CONTROL REQUIREMENTS	
The organization includes practical exercises in security awareness training that simulate actual cyber-attacks.	
AGENCY IMPLEMENTATION STANDARDS	
Std.01 — DFPS Office of Information Security will periodically conduct phishing campaigns by sending simulated phishing emails to information resource users. Std.02 – DFPS Office of Information Security may assign the user role-based training, depending on his or her role at DFPS, to better understand targeted phishing attacks.	
SUPPLEMENTAL GUIDANCE	
Practical exercises may include, for example, no-notice social engineering attempts to collect information, gain unauthorized access, or simulate the adverse impact of opening malicious email attachments or invoking, via spear phishing attacks, malicious web links.	
REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Phishing Security Awareness Training; **Federal**: NIST SP 800-12, 800-30, 800-39, 800-50, 800-100;	PM-12.
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System security plan; privacy plan; security awareness and training policy; procedures addressing security awareness training implementation; security awareness training curriculum; security awareness training materials; other relevant documents or records. Interview: Organizational personnel who participate in security awareness training; organizational personnel with responsibilities for security awareness training; organizational personnel with information security responsibilities. Test: Automated mechanisms implementing cyber-attack simulations in practical exercises.	

AT-02(02): INSIDER THREAT

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CJIS
CONTROL REQUIREMENTS	

The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Security awareness training includes content on insider threat in training for employees and contractors in accordance with PM-12.

Security awareness training includes training on recognizing and reporting potential indicators of insider threat, such as:

a. Inordinate, long-term job dissatisfaction;
b. Attempts to gain access to information not required for job performance;
c. Unexplained access to financial resources;
d. Bullying or sexual harassment of fellow employees;
e. Workplace violence; and
f. Other serious violations of organizational policies, procedures, directives, rules, or practices.

SUPPLEMENTAL GUIDANCE

Potential indicators and possible precursors of insider threat can include behaviors such as inordinate, long-term job dissatisfaction; attempts to gain access to information not required for job performance; unexplained access to financial resources; bullying or harassment of fellow employees; workplace violence; and other serious violations of policies, procedures, directives, regulations, rules, or practices. Literacy training includes how to communicate the concerns of employees and management regarding potential indicators of insider threat through channels established by the organization and in accordance with established policies and procedures. Organizations may consider tailoring insider threat awareness topics to the role. For example, training for managers may be focused on changes in the behavior of team members, while training for employees may be focused on more general observations.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; Employee Safety and Security Awareness (CAPPS); DFPS Safety Policy (HR-1107); DFPS Worker Safety Support Training; DFPS Office and Building Safety; **Federal**: NIST SP 800-50, 800-160-2, 800-181; FBI CJIS CSP v5.9	PM-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System security plan; privacy plan; literacy training and awareness policy; procedures addressing literacy training and awareness implementation; literacy training and awareness curriculum; literacy training and awareness materials; other relevant documents or records.

Interview: Organizational personnel who participate in literacy training and awareness; organizational personnel with responsibilities for literacy training and awareness; organizational personnel with information security and privacy responsibilities.

AT-03: ROLE-BASED SECURITY TRAINING

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Provide role-based security and privacy training to personnel with the following roles and responsibilities: Cybersecurity and/or Information Security Analyst
   1. Before authorizing access to the system, information, or performing assigned duties, and when an employee enters a new position that requires additional role-specific training, and annually thereafter; and
   2. When required by system changes;
b. Update role-based training content annually and following major changes to legislation or security Requirements; and
c. Incorporate lessons learned from internal or external security incidents or breaches into role-based training.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS will provide role-based information security training to staff with significant information security roles and responsibilities to undergo appropriate information system security training prior to authorizing access to DFPS networks, systems, and/or applications; when required by significant information system or system environment changes; and when an employee enters a new position that requires additional role-specific training and refresher training within every three hundred sixty-five (365) days thereafter. [Source: DIR Control Standards Catalog AT-3]

Std.02 — The DFPS Commissioner or his/her designated representative(s) will ensure that the agency has trained personnel to assist the agency in complying with the requirements of 1 TAC 202 and related policies. [Source: 1 TAC 202.20(4)]

Std.03 — DFPS Chief Information Security Officer is responsible for providing training and direction for personnel with significant responsibilities for information security with respect to such responsibilities. [Source: 1 TAC 202.21(b)(4)]

Std.04 — DFPS may spend public funds as appropriate to reimburse a state agency employee or administrator who serves in an information technology, cybersecurity, or other cyber-related position for fees associated with industry-recognized certification examinations. [Source: TX Govt. Code 656.047(a)(1)]

Std.05 — DFPS shall comply with the mandatory guidelines provided by DIR regarding the initial and continuing education requirements needed for cybersecurity training that must be completed by all information resources employees of the agencies. [Source: TX Govt. Code 2054.076(b)]

Std.06 — DFPS shall, with available funds, identify information security issues and develop a plan to prioritize the remediation of those issues. The agency shall include in the plan:

a. Analysis of the percentage of state agency personnel in information technology, cybersecurity, or other cyber-related positions who currently hold the appropriate industry-recognized certifications as identified by the National Initiative for Cybersecurity Education; and
b. The level of preparedness of DFPS cyber personnel and potential personnel who do not hold the appropriate industry-recognized certifications to successfully complete the industry- recognized certification examinations; and
c. A strategy for mitigating any workforce-related discrepancy in information technology, cybersecurity, or other cyber-related positions with the appropriate training and industry- recognized certifications. [Source: TX Govt. Code 2054.575(a)(3, 4, 5)]

SUPPLEMENTAL GUIDANCE

Organizations determine the appropriate content of security training based on the assigned roles and responsibilities of individuals and the specific security requirements of DFPS and the information systems to which personnel have authorized access. In addition, organizations provide enterprise architects, information system developers, software developers, acquisition/procurement officials, information system managers, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security-related technical training specifically tailored for their assigned duties.

Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. Such training can include for example, policies, procedures, tools, and artifacts for the organizational security roles defined. Organizations also provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of DFPS's information security programs.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Information Security Program Policy **State:** 1 TAC 202.20(4), 1 TAC 202.21(b)(4); TX Govt. Code 656.047, TX Govt. Code 2054.076;DIR Information Resources Employees Continuing Education Guidelines for Cybersecurity; DIR Security Control Standards Catalog **Federal:** NIST SP 800-50, 800-181; FBI CJIS CSP v5.9	AC-3, AC-17, AC-22, AT-2, AT-4, CP-3, IR-2, IR-4, IR-7, IR-9, PL-4, PM-13, PM-23, PS-7, PS-9, SA-3, SA-8, SA-11, SA-16, SR-5, SR-6, SR-11.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System security plan; privacy plan; security and privacy awareness and training policy; procedures addressing security and privacy training implementation; codes of federal regulations; security and privacy training curriculum; security and privacy training materials; training records; other relevant documents or records.

Interview: Organizational personnel with responsibilities for role-based security and privacy training; organizational personnel with assigned system security and privacy roles and responsibilities.

Test: Automated mechanisms managing role-based security and privacy training.

AT-04: SECURITY TRAINING RECORDS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and

b. Retain individual training records for termination of employment + five years.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS maintains training records consistent with State and Agency defined retention policies.

SUPPLEMENTAL GUIDANCE

Documentation for specialized training may be maintained by individual supervisors at the discretion of the organization. The National Archives and Records Administration provides guidance on records retention for federal agencies.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Human Resources Manual Chapter 14: Employment Records (F. Other Personnel Records). **State:** 1 TAC 202.20(4), 1 TAC 202.21(b)(4); TX Govt. Code 656.047, TX Govt. Code 2054.076;DIR Information Resources Employees Continuing Education Guidelines for Cybersecurity; DIR Security Control Standards Catalog **Federal:** FBI CJIS CSP v5.9	AT-2, AT-3, CP-3, IR-2, PM-14, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System security plan; privacy plan; security and privacy awareness and training policy; procedures addressing security and privacy training implementation; codes of federal regulations; security and privacy training curriculum; security and privacy training materials; training records; other relevant documents or records.

Interview: Organizational personnel with responsibilities for role-based security and privacy training; organizational personnel with assigned system security and privacy roles and responsibilities.

Test: Automated mechanisms managing role-based security and privacy training.

(AU) AUDIT AND ACCOUNTABILITY

The DFPS organization requires the creation, protection, and retention of information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity. The DFPS organization requires that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

The AU control family consists of security controls related to DFPS audit capabilities. This includes audit policies and procedures, audit logging, audit report generation, and protection of audit information. The intended audience for this Control includes, but is not limited to, information resource owners and custodians. Information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented.

AU-01: AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Develop, document, and disseminate to appropriate personnel:
   1. Organization-level audit and accountability policy that:
      a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
b. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls;
c. Designate a senior management official as defined in the audit and accountability policy to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; and
d. Review and update the current audit and accountability:
   1. Policy every year and following major changes to legislation or security requirements; and
   2. Procedures every year and following major changes to legislation or security requirements.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS Office of Information Security will develop, disseminate, and periodically review/update formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls. [Source: DIR Control Standards Catalog AU-1]

Std.02 — The DFPS Chief Information Security Officer is responsible for:

a. Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks;
b. Providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities under 1 TAC 202; and
c. Developing and recommending policies and establishing procedures and practices, in cooperation with the agency Information Resources Manager, information-owners and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, or disclosure. [Source: 1 TAC 202.21(b)(3, 5, 8)]

SUPPLEMENTAL GUIDANCE

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AU family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

REFERENCES	RELATED CONTROLS

Agency: DFPS Information Security Policy; DFPS Information Security Program Policy. **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP 800-12, 800-30, 800-39, 800-10	AC-3, AC-17, AC-22, AT-2, AT-4, CP-3, IR-2, IR-4, IR-7, IR-9, PL-4, PM-13, PM-23, PS-7, PS-9, SA-3, SA-8, SA-11, SA-16, SR-5, SR-6, SR-11.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Audit and accountability policy and procedures; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with audit and accountability responsibilities; organizational personnel with information security and privacy responsibilities.

AU-02: AUDIT EVENTS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Identifies the types of auditable events listed in the DFPS Auditable Events Standard that the system is capable of logging in support of the audit function;
b. Coordinates the event logging function with other organizational entities requiring audit-related information to guide and inform the selection of auditable events to be logged;
c. Specifies the types of events that will be logged within the system along with the frequency of (or situation requiring) logging for each identified event type;
d. Provides a rationale for why the types of events selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and
e. Reviews and update the types of events selected for logging at least annually.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Information resources systems must provide the means whereby authorized personnel have the ability to audit and establish individual accountability for any action that can potentially cause access to, generation of, modification of, or affect the release of confidential information. [Source: DIR Control Standards Catalog AU-2]

Std.02 — Appropriate audit trails must be maintained to provide accountability for updates to mission critical information, hardware, and software and for all changes to automated security or access rules. [Source: DIR Control Standards Catalog AU-2]

Std.03 — Based on the risk assessment, a sufficiently complete history of transactions must be maintained to permit an audit of the information resources system by logging and tracing the activities of individuals through the system. [Source: DIR Control Standards Catalog AU- 2]

Std.04 — If capable, systems must log the following event types:

a. Authentication events:

b. File and Objects events:
c. Writes/downloads to devices/media (for example, floppy disks, CD/DVD drives, USB devices/printers) (Success/Failure)
d. Uploads from devices/media (for example, USB, CD/DVD drives (Success/Failure)
e. User and Group Management events:
f. Use of Privileged/Special Rights events
g. Admin or root-level access (Success/Failure)
h. Privilege/Role escalation (Success/Failure)
i. Audit and log data accesses (Success/Failure)
j. System reboot, restart, and shutdown (Success/Failure)
k. Print to a device (Success/Failure)
l. Print to a file (for example, pdf format) (Success/Failure)
m. Application (for example, Firefox, Internet Explorer, MS Office Suite, etc.) initialization (Success/Failure)
n. Export of information (Success/Failure) include (for example, to CDRW, thumb drives, or remote systems)
o. Import of information (Success/Failure) include (for example, from CDRW, thumb drives, or remote systems)

Std.05 — Event logs must be retained in a format that allows compilation of auditing records from multiple components into a system-wide, time-correlated audit trail.

Std.06 — At a minimum, the list of auditable events for a system must be adequate to support after-the-fact investigations of security events. Event logging plans for a system must be updated following any investigation where a deficiency of auditing is uncovered for a similar system.

SUPPLEMENTAL GUIDANCE

An event is an observable occurrence in a system. The types of events that require logging are those events that are significant and relevant to the security of systems and the privacy of individuals. Event logging also supports specific monitoring and auditing needs. Event types include password changes, failed logons or failed accesses related to systems, security or privacy attribute changes, administrative privilege usage, PIV credential usage, data action changes, query parameters, or external credential usage. In determining the set of event types that require logging, organizations consider the monitoring and auditing appropriate for each of the controls to be implemented. For completeness, event logging includes all protocols that are operational and supported by the system.

To balance monitoring and auditing requirements with other system needs, event logging requires identifying the subset of event types that are logged at a given point in time. For example, organizations may determine that systems need the capability to log every file access successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance. The types of events that organizations desire to be logged may change. Reviewing and updating the set of logged events is necessary to help ensure that the events remain relevant and continue to support the needs of the organization. Organizations consider how the types of logging events can reveal information about individuals that may give rise to privacy risk and how best to mitigate such risks. For example, there is the potential to reveal personally identifiable information in the audit trail, especially if the logging event is based on patterns or time of usage.

Event logging requirements, including the need to log specific event types, may be referenced in other controls and control enhancements. These include AC-02(04), AC- 06(09), AC-17(01), CM-03f, CM-05(01), PE-03, PM-21, PT-07, and RA-08. Organizations

include event types that are required by applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. Audit records can be generated at various levels, including at the packet level as information traverses the network. Selecting the appropriate level of event logging is an important part of a monitoring and auditing capability and can identify the root causes of problems. When defining event types, organizations consider the logging necessary to cover related event types, such as the steps in distributed, transaction-based processes and the actions that occur in service-oriented architectures.

REFERENCES	**RELATED CONTROLS**

Agency: DFPS Information Security Policy; DFPS IT Systems Auditable Events Policy. **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP 800-92; FBI CSP v5.9 Section 5.4.1	AC-2, AC-3, AC-6, AC-7, AC-8, AC-16, AC-17, AU-3, AU-4, AU-5, AU-6, AU-7, AU-11, AU-12, CM-3, CM-5, CM-6, CM-13, IA-3, MA-4, MP-4, PE-3, PM-21, PT-2, PT-7, RA-8, SA-8, SC-7, SC-18, SI-3, SI-4, SI-7, SI-10, SI-11.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Audit and accountability policy; procedures addressing auditable events; system security plan; privacy plan; system design documentation; system configuration settings and associated documentation; system audit records; system auditable events; other relevant documents or records.

Interview: Organizational personnel with audit and accountability responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators.

Test: Automated mechanisms implementing system auditing.

AU-03: CONTENT OF AUDIT RECORDS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

Ensure that audit records contain information that establishes the following:

a. What type of event occurred;
b. When the event occurred;
c. Where the event occurred;
d. Source of the event;
e. Outcome of the event; and
f. Identity of any individuals, subjects, or objects/entities associated with the event

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Audit record content must follow the DFPS Auditable Event policy to include:

a. Date and time of the event;

b. The component of the information system (e.g., software component, hardware component) where the event occurred;

c. Type of event;

d. User/subject identity; and

e. The outcome (success or failure) of the event.

[Source: DIR Control Standards Catalog AU-3]

Std.02 — For moderate and high-security baseline systems, the audit function must have the capability of providing more detailed information for audit events identified by type, location, or subject as required by DFPS.

Std.03 — Raw audit records must be available in an unaltered format.

SUPPLEMENTAL GUIDANCE

Audit record content that may be necessary to support the auditing function includes event descriptions (item a), time stamps (item b), source and destination addresses (item c), user or process identifiers (items d and f), success or fail indications (item e), and filenames involved (items a, c, e, and f) . Event outcomes include indicators of event success or failure and event-specific results, such as the system security and privacy posture after the event occurred. Organizations consider how audit records can reveal information about individuals that may give rise to privacy risks and how best to mitigate such risks. For example, there is the potential to reveal personally identifiable information in the audit trail, especially if the trail records inputs or is based on patterns or time of usage.

NIST Special Publication 800-92 provides guidance on computer security log management. [Source: DIR Control Standards Catalog AU-3]

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS IT Systems Auditable Events Policy. **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP 800-92; NIST IR 8062; FBI CSP v5.9 Section 5.4.1	AU-2, AU-8, AU-12, AU-14, MA-4, PL-9, SA-8, SI-7, SI-11.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Audit and accountability policy; system security plan; privacy plan; procedures addressing content of audit records; system design documentation; system configuration settings and associated documentation; list of organization-defined auditable events; system audit records; system incident reports; other relevant documents or records.

Interview: Organizational personnel with audit and accountability responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators.

Test: Automated mechanisms implementing system auditing.

AU-03(01): ADDITIONAL AUDIT INFORMATION

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

Generate audit records containing the following additional information: as defined in Std.02 below, sufficient information to support after-the-fact investigation.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. [Source: SP 800-171 3.3.1]

Std.02 — Additional information must be limited to that explicitly needed for specific audit requirements. Systems must be configured to generate audit records containing the following additional elements as feasible:

a. Filename accessed;
b. Program or command used to initiate the event;
c. Manufacturer-specific event name/type of event;
d. Source and destination network addresses;
e. Source and destination port or protocol identifiers;
f. Other security-relevant actions associated with processing; and
g. Any additional significant system events or risks.

SUPPLEMENTAL GUIDANCE

The ability to add information generated in audit records is dependent on system functionality to configure the audit record content. Organizations may consider additional information in audit records including, but not limited to, access control or flow control rules invoked and individual identities of group account users. Organizations may also consider limiting additional audit record information to only information that is explicitly needed for audit requirements. This facilitates the use of audit trails and audit logs by not including information in audit records that could potentially be misleading, make it more difficult to locate information of interest, or increase the risk to individuals' privacy.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS IT Systems Auditable Events Policy. **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP 800-92; NIST IR 8062; FBI CSP v5.9 Section 5.4.1	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Audit and accountability policy; procedures addressing content of audit records; system security plan; privacy plan; system design documentation; system configuration settings and associated documentation; list of organization-defined auditable events; system audit records; other relevant documents or records.

Interview: Organizational personnel with audit and accountability responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators; system developers.

Test: System audit capability

AU-04: AUDIT STORAGE CAPACITY

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

Allocate audit log storage capacity to accommodate audit log retention requirements as defined in the Records Retention Schedule.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Allocate sufficient audit record storage capacity and configure auditing to reduce the likelihood of such capacity being exceeded even during peak performance times. [Source: DIR Control Standards Catalog AU-4]

SUPPLEMENTAL GUIDANCE

Organizations consider the types of audit logging to be performed and the audit log processing requirements when allocating audit log storage capacity. Allocating sufficient audit log storage capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of audit logging capability.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS IT Systems Auditable Events Policy. **State:** DIR Security Control Standards Catalog. **Federal:** FBI CSP v5.9 Section 5.4.6	AU-2, AU-5, AU-6, AU-7, AU-9, AU-11, AU-12, AU-14, SI-4.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Organizational personnel with audit and accountability responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators; system developers.

Interview: Audit record storage capacity and related configuration settings.

AU-05: RESPONSE TO AUDIT PROCESSING FAILURES

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

a. Alert personnel or roles as identified in the System Security Plan (SSP) within 30 minutes in the event of an audit logging process failure; and
b. Take the following additional actions: actions as outlined in the SSP.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — The information system must alert appropriate organizational officials in the event of an audit processing failure. [Source: DIR Control Standards Catalog AU-5]

SUPPLEMENTAL GUIDANCE

Audit logging process failures include software and hardware errors, failures in audit log capturing mechanisms, and reaching or exceeding audit log storage capacity. Organization- defined actions include overwriting oldest audit records, shutting down the system, and stopping the generation of audit records. Organizations may choose to define additional actions for audit logging process failures based on the type of failure, the location of the failure, the severity of the failure, or a combination of such factors. When the audit logging process failure is related to storage, the response is carried out for the audit log storage repository (i.e., the distinct system component where the audit logs are stored), the system on which the audit logs reside, the total audit log storage capacity of the organization (i.e., all audit log storage repositories combined), or all three. Organizations may decide to take no additional actions after alerting designated roles or personnel.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS IT Systems Auditable Events Policy. **State:** DIR Security Control Standards Catalog. **Federal:** FBI CSP v5.9 Section 5.4.2	AU-2, AU-4, AU-7, AU-9, AU-11, AU-12, AU-14, SI-4, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Audit and accountability policy; procedures addressing response to audit processing failures; system design documentation; system security plan; privacy plan; system configuration settings and associated documentation; list of personnel to be notified in case of an audit processing failure; system audit records; other relevant documents or records.

Interview: Organizational personnel with audit and accountability responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators; system developers.

Test: Automated mechanisms implementing system response to audit processing failures.

AU-05(01): RESPONSE TO AUDIT PROCESSING FAILURES

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

a. The information system that process CJI provides alert personnel or roles as identified in the System Security Plan (SSP) within 60 minutes in the event of an audit logging process failure; and

b. The information system that processes CJI provides alert personnel or roles as identified in the System Security Plan (SSP) within 60 minutes when allocated audit record storage volume reaches the defined percentage of repository maximum audit record storage capacity.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — The information system must alert appropriate organizational officials in the event of an audit processing failure as defined in the System Security Plan (SSP)

SUPPLEMENTAL GUIDANCE

Organizations may have multiple audit data storage repositories distributed across multiple information system components, with each repository having different storage volume capacities.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS IT Systems Auditable Events Policy. **State:** DIR Security Control Standards Catalog. **Federal:** FBI CSP v5.9 Section 5.4.2	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Audit and accountability policy; procedures addressing response to audit processing failures; system design documentation; system security plan; privacy system configuration settings and associated documentation; system audit records; other relevant documents or records.

Interview: Organizational personnel with audit and accountability responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators; system developers.

Test: Automated mechanisms implementing audit storage limit warnings.

AU-05(02): REAL-TIME ALERTS

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The information system that process CJI alerts in real-time to personnel or roles as identified in the System Security Plan (SSP) when the following audit failure events occur:

a. Record log is full;
b. Auditing application reports an error;
c. Authentication logging failure; and
d. Encryption logging failure.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — The information system must alert appropriate organizational officials in the event of an audit processing failure as defined in the System Security Plan (SSP)

SUPPLEMENTAL GUIDANCE

Alerts provide organizations with urgent messages. Real-time alerts provide these messages at information technology speed (i.e., the time from event detection to alert occurs in seconds or less).

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS IT Systems Auditable Events Policy. **Federal:** FBI CSP v5.9 Section 5.4.2	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Audit and accountability policy; procedures addressing response to audit processing failures; system design documentation; system security plan; privacy plan; system configuration settings and associated documentation; system audit records; other relevant documents or records.

Interview: Organizational personnel with audit and accountability responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators; system developers.

AU-06: AUDIT REVIEW, ANALYSIS, AND REPORTING

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Reviews and analyzes information system audit records for indication of inappropriate or unusual activity in accordance with the DFPS IT Systems Auditable Events Policy;

b. Reports findings to defined personnel or roles (defined in the applicable system security plan);

c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Regularly review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions. [Source: DIR Control Standards Catalog AU-6]

Std.02 —

a. Comply with all relevant legal requirements applicable to monitoring activities. Items that are monitored include:

1. Authorized access; and
2. Unauthorized access attempts.

b. Specify how often audit logs are reviewed, how the reviews are documented, and the specific roles and responsibilities of the personnel conducting the reviews, including the professional certifications or other qualifications required.

c. Periodically test monitoring and detection processes, remediate deficiencies, and improve processes. [Source: Hitrust 09.ab Monitoring System Use]

Std.03 — Ensure that proper logging is enabled in order to audit administrator activities. Review system administrator and operator logs on a regular basis. [Source: Hitrust 09.ad Administrator and Operator Logs]

Std.04 — Audit records must be reviewed by the information resource custodian on a routine basis, or immediately upon receipt of an alert event. Any alert events that indicate suspicious behavior must be reported to the DFPS chief information security officer as a potential security incident immediately upon discovery.

SUPPLEMENTAL GUIDANCE

Audit record review, analysis, and reporting covers information security- and privacy-related logging performed by organizations, including logging that results from the monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and non-local maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at system interfaces, and use of mobile code or Voice over Internet Protocol (VoIP). Findings can be reported to organizational entities that include the incident response team, help desk, and security or privacy offices. If organizations are prohibited from reviewing and analyzing audit records or unable to conduct such activities, the review or analysis may be carried out by other organizations granted such authority. The frequency, scope, and/or depth of the audit record review, analysis, and reporting may be adjusted to meet organizational needs based on new information received.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS IT Systems Auditable Events Policy. **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP 800-86, 800-101; FBI CSP v5.9 Section 5.4.2	AC-2, AC-3, AC-5, AC-6, AC-7, AC-17, AU-7, AU-16, CA-2, CA-7, CM-2, CM-5, CM-6, CM-10, CM-11, IA-2, IA-3, IA-5, IA-8, IR-5, MA-4, MP-4, PE-3, PE-6, RA-5, SA-8, SC-7, SI-3, SI-4, SI-7.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Audit and accountability policy; system security plan; privacy plan; procedures addressing audit review, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; other relevant documents or records.

Interview: Organizational personnel with audit review, analysis, and reporting responsibilities; organizational personnel with information security and privacy responsibilities.

AU-06(01): AUTOMATED PROCESS INTEGRATION

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

Integrate audit record review, analysis, and reporting processes using automated mechanisms as identified in System Security Plans (SSPs) to support organizational processes for investigation and response to suspicious activities.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Ensure that appropriate records are aggregated to a centralized security information and event management (SIEM) or centralized audit repository for analysis and review by DFPS Office of Information Security:

a. Information is provided to DFPS Office of Information Security in a searchable format compliant with DFPS, state, and federal requirements;
b. Audit record sources include systems, appliances, devices, services, and applications (including databases); and
c. DFPS Office of Information Security-directed audit information collection rules/requests (for example, sources, queries, data calls) are implemented/provided within the timeframe specified in the request.

Std.02 — Raw audit records and raw security information/results from relevant automated tools must be available in an unaltered format to DFPS Office of Information Security.

SUPPLEMENTAL GUIDANCE

Organizational processes benefiting from integrated audit review, analysis, and reporting include, for example, incident response, continuous monitoring, contingency planning, and Inspector General audits.

REFERENCES	RELATED CONTROLS

Agency: DFPS Information Security Policy; DFPS IT Systems Auditable Events Policy. **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP 800-86, 800-101; FBI CSP v5.9 Section 5.3.2.2, 5.3.4, 5.4.2	PM-7.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Audit and accountability policy; system security plan; privacy plan; procedures addressing audit review, analysis, and reporting; procedures addressing investigation and response to suspicious activities; system design documentation; system configuration settings and associated documentation; system audit records; other relevant documents or records.

Interview: Organizational personnel with audit review, analysis, and reporting responsibilities; organizational personnel with information security and privacy responsibilities.

Test: Automated mechanisms integrating audit review, analysis, and reporting processes.

AU-06(03): CORRELATE AUDIT REPOSITORIES

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Correlated results from automated tools must be searchable by DFPS Office of Information Security:

a. Information is provided to DFPS Office of Information Security in a format compliant with DFPS, state, and Federal (for example, Continuous Diagnostics and Mitigation) requirements;
b. Repository sources include systems, appliances, devices, services, and applications (including databases); and
c. DFPS Office of Information Security directed repository information collection rules/requests (for example, sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.

SUPPLEMENTAL GUIDANCE

Organization-wide situational awareness includes awareness across all three tiers of risk management (i.e., organizational, mission/business process, and information system) and supports cross-organization awareness.

REFERENCES	**RELATED CONTROLS**

Agency: DFPS Information Security Policy; DFPS IT Systems Auditable Events Policy. **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP 800-86, 800-101; FBI CSP v5.9 Section 5.4.1, 5.4.3,	AU-12, IR-4.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Audit and accountability policy; system security plan; privacy plan; procedures addressing audit review, analysis, and reporting; system design documentation; system configuration settings and associated documentation; system audit records across different repositories; other relevant documents or records.

Interview: Organizational personnel with audit review, analysis, and reporting responsibilities; organizational personnel with information security and privacy responsibilities.

Test: Automated mechanisms supporting analysis and correlation of audit records.

AU-07: AUDIT REDUCTION AND REPORT GENERATION

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The information system provides an audit reduction and report generation capability that:

a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and

b. Does not alter the original content or time marking of audit records.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Configure security information and event management (SIEM) tools and systems to provide audit reduction and report generation capabilities that support near real-time audit review and after-the-fact investigations based on selectable event criteria in accordance with AU-06.

Std.02 — Ensure that audit record processing does not degrade the operational performance of the control system. [Source: Catalog of Control Systems Security: Recommendations for Standards Developers]

SUPPLEMENTAL GUIDANCE

Audit record reduction is a process that manipulates collected audit log information and organizes it into a summary format that is more meaningful to analysts. Audit record reduction and report generation capabilities do not always emanate from the same system or from the same organizational entities that conduct audit logging activities. The audit record reduction capability includes modern data mining techniques with advanced data filters to identify anomalous behavior in audit records. The report generation capability provided by the system can generate customizable reports. Time ordering of audit records can be an issue if the granularity of the timestamp in the record is insufficient.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Auditable Events Standard; DFPS Auditable Events Policy **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP 800-86, 800-101; FBI CSP v5.9 Section 5.4.3	AC-2, AU-2, AU-3, AU-4, AU-5, AU-6, AU-12, AU-16, CM-5, IA-5, IR-4, PM-12, SI-4.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Audit and accountability policy; system security plan; privacy plan; procedures addressing audit reduction and report generation; system design documentation; system configuration settings and associated documentation; audit reduction, review, analysis, and reporting tools; system audit records; other relevant documents or records.

Interview: Organizational personnel with audit reduction and report generation responsibilities; organizational personnel with information security and privacy responsibilities.

Test: Audit reduction and report generation capability.

AU-08: TIME STAMPS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The information system:

a. Uses internal system clocks to generate time stamps for audit records; and

b. Record time stamps for audit records that meet the degree of synchronization between systems and reference clocks as defined in the System Security Plan (SSP) based on the sensitivity of the system, at minimum within 1 second of accuracy and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Whenever technically possible, information systems should provide time stamps for use in audit record generation. [Source: DIR Control Standards Catalog AU-8]

Std.02 — The agency will synchronize internal information system clocks on an annual basis. [Source: FBI CJIS Security Policy]

SUPPLEMENTAL GUIDANCE

Time stamps generated by the information system include date and time. Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an

offset from UTC. Granularity of time measurements refers to the degree of synchronization between information system clocks and reference clocks, for example, clocks synchronizing within hundreds of milliseconds or within tens of milliseconds. Organizations may define different time granularities for different system components. Time service can also be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** FBI CJIS CSP v5.9	AU-3, AU-12, AU-14, SC-45.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Audit and accountability policy; system security plan; privacy plan; procedures addressing timestamp generation; system design documentation; system configuration settings and associated documentation; system audit records; other relevant documents or records.

Interview: Organizational personnel with information security and privacy responsibilities; system/network administrators; system developers.

Test: Automated mechanisms implementing timestamp generation.

AU-08(01): SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

This control is withdrawn and moved to SC-45(01) but still referenced in the FBI CJIS Security Policy v5.9. Please see SC-45(01).

AU-09: PROTECTION OF AUDIT INFORMATION

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The information system:

a. Protects audit information and audit logging tools from unauthorized access, modification, and deletion; and

b. Alert personnel or roles as specified in System Security Plans (SSPs) upon detection of unauthorized access, modification, or deletion of audit information.

AGENCY IMPLEMENTATION STANDARDS

Std.01 —The information system must protect audit information and audit tools from unauthorized access, modification, and deletion. [Source: DIR Control Standards Catalog AU- 9]

SUPPLEMENTAL GUIDANCE

Audit information includes all information needed to successfully audit system activity, such as audit records, audit log settings, audit reports, and personally identifiable information.

Audit logging tools are those programs and devices used to conduct system audit and logging activities. Protection of audit information focuses on technical protection and limits the ability to access and execute audit logging tools to authorized individuals. Physical protection of audit information is addressed by both media protection controls and physical and environmental protection controls.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Auditable Events Standard; DFPS Auditable Events Policy **State:** DIR Security Control Standards Catalog. **Federal:** FIPS 140, 180, 202; FBI CSP v5.9 Section 5.3.4, 5.4.5	AC-3, AC-6, AU-6, AU-11, AU-14, AU-15, MP-2, MP-4, PE-2, PE-3, PE-6, SA-8, SC-8, SI-4.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Audit and accountability policy; system security plan; privacy plan; access control policy and procedures; procedures addressing protection of audit information; system design documentation; system configuration settings and associated documentation; system audit records; audit tools; other relevant documents or records.

Interview: Organizational personnel with audit and accountability responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators; system developers.

Test: Mechanisms implementing audit information protection.

AU-09(02): AUDIT BACKUP ON SEPARATE PHYSICAL SYSTEMS/COMPONENTS

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The information system backs up audit records per the organization-defined frequency onto a physically different system or system component than the system or component being audited.

AGENCY IMPLEMENTATION STANDARDS

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.01 — The information system backs up audit records to the frequency defined in the System Security Plan (SSP) onto a physically different system (e.g. central audit server) or system component than the system or component being audited.

SUPPLEMENTAL GUIDANCE

This control enhancement helps to ensure that a compromise of the information system being audited does not also result in a compromise of the audit records.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Auditable Events Standard; DFPS Auditable Events Policy **State:** DIR Security Control Standards Catalog. **Federal:** FIPS 140, 180, 202; FBI CSP v5.9 Section 5.4.6	AU-4, AU-5.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Audit and accountability policy; system security plan; privacy plan; procedures addressing protection of audit information; system design documentation; system configuration settings and associated documentation; system or media storing backups of system audit records; system audit records; other relevant documents or records.

Interview: Organizational personnel with audit and accountability responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators; system developers.

Test: Automated mechanisms implementing the backing up of audit records.

AU-09(04): ACCESS BY SUBSET OF PRIVILEGED USERS

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

Authorize access to management of audit logging functionality to only the subset of privileged users or roles identified in the System Security Plan (SSP).

AGENCY IMPLEMENTATION STANDARDS

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.01 — Restrict access to audit logging functionality to system owners, authorized system administrators, designated security officials, and others with a valid business need and who are not subject to auditing by the system. System and network administrators must not have the ability to modify or delete audit log entries.

SUPPLEMENTAL GUIDANCE

Individuals or roles with privileged access to a system and who are also the subject of an audit by that system may affect the reliability of the audit information by inhibiting audit activities or modifying audit records. Requiring privileged access to be further defined between audit-related privileges and other privileges limits the number of users or roles with audit-related privileges.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Auditable Events Standard; DFPS Auditable Events Policy **State:** DIR Security Control Standards Catalog. **Federal:** FIPS 140, 180, 202; FBI CSP v5.9 Section 5.4.5	AU-5.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Audit and accountability policy; system security plan; privacy plan; procedures addressing protection of audit information; system design documentation; system configuration settings and associated documentation; system or media storing backups of system audit records; system audit records; other relevant documents or records.

Interview: Organizational personnel with audit and accountability responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators; system developers.

Test: Automated mechanisms implementing the backing up of audit records.

AU-10: NON-REPUDIATION

Priority: P1

Baseline(s): High	Overlay(s): DIR

CONTROL REQUIREMENTS

The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed a particular action.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Enable auditing sufficient to uniquely identify actors, actions, times of actions, and devices associated with actions (see AU-03).

SUPPLEMENTAL GUIDANCE

Types of individual actions covered by non-repudiation include creating information, sending, and receiving messages, and approving information. Non-repudiation protects against claims by authors of not having authored certain documents, senders of not having transmitted messages, receivers of not having received messages, and signatories of not having signed documents. Non-repudiation services can be used to determine if information originated from an individual or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request, or receiving specific information).

Organizations obtain non-repudiation services by employing various techniques or mechanisms, including digital signatures and digital message receipts.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Auditable Events Standard; DFPS Auditable Events Policy **State:** DIR Security Control Standards Catalog. **Federal:** FIPS 140, 180, 186, 202; NIST SP 800-177	AU-9, PM-12, SA-8, SC-8, SC-12, SC-13, SC-16, SC-17, SC-23.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Audit and accountability policy; system security plan; privacy plan; procedures addressing non-repudiation; system design documentation; system configuration settings and associated documentation; system audit records; other relevant documents or records.

Interview: Organizational personnel with audit and accountability responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators; system developers.

Test: Automated mechanisms implementing non-repudiation capability.

AU-11: AUDIT RECORD RETENTION

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

Retain audit records for a time period consistent with DFPS Records Retention schedule, not less than one year, to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS must retain audit records to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. [Source: DIR Control Standards Catalog AU-11]

Std.02 — Audit records include system, application, and database-level audit logs and logs for network devices. Where possible, audit records should be retained for 90 days online, after which they may be stored offline or transferred from remote access devices to a central log server for a period not less than one year.

Std.03 — When subject to a legal investigation, audit records must be maintained until released by the investigating authority. After release, maintain audit records in accordance with the records retention schedule.

Std.04 — Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. [Source: SP 800-171 3.3.1]

Std.05 — Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions. [Source: SP 800-171 3.3.2]

SUPPLEMENTAL GUIDANCE

Organizations retain audit records until it is determined that the records are no longer needed for administrative, legal, audit, or other operational purposes. This includes the retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoenas, and law enforcement actions. Organizations develop standard categories of audit records relative to such types of actions and standard response processes for each type of action. The National Archives and Records Administration (NARA) General Records Schedules provide federal policy on records retention.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Auditable Events Standard; DFPS Auditable Events Policy **State:** DIR Security Control Standards Catalog. **Federal:** FIPS 140, 180, 186, 202; NIST SP 800-177; FBI CJIS CSP v5.9	AU-2, AU-4, AU-5, AU-6, AU-9, AU-14, MP-6, RA-5, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Audit and accountability policy; system security plan; privacy plan; audit record retention policy and procedures; security plan; organization-defined retention period for audit records; audit record archives; audit logs; audit records; other relevant documents or records.

Interview: Organizational personnel with audit and accountability responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators.

AU-12: AUDIT GENERATION

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The information system:

a. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-02a on all information systems and system components where audit capability exists;

b. Allow designated personnel or roles as identified in the System Security Plan (SSP) to select the event types that are to be logged by specific components of the system; and

c. Generate audit records for the event types defined in AU-02c that include the audit record content defined in AU-03.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS must configure information systems to generate audit records to support AU-02 and AU-03. [Source: DIR Control Standards Catalog AU-12]

Std.02 — Where feasible, systems must provide the capability to compile audit records from multiple components into a system-wide (logical or physical) audit trail that is time- correlated to within acceptable tolerances between time stamps of individual records in the audit trail.

SUPPLEMENTAL GUIDANCE

Organizations retain audit records until it is determined that the records are no longer needed for administrative, legal, audit, or other operational purposes. This includes the retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoenas, and law enforcement actions. Organizations develop standard categories of audit records relative to such types of actions and standard response processes for each type of action. The National Archives and Records Administration (NARA) General Records Schedules provide federal policy on records retention.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Auditable Events Standard; DFPS Auditable Events Policy **State:** DIR Security Control Standards Catalog. **Federal:** FBI CJIS CSP v5.9	AC-6, AC-17, AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-14, CM-5, MA-4, MP-4, PM-12, SA-8, SC-18, SI-3, SI-4, SI-7, SI-10.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Audit and accountability policy; procedures addressing audit record generation; system security plan; privacy plan; system design documentation; system configuration settings and associated documentation; list of auditable events; system audit records; other relevant documents or records.

Interview: Organizational personnel with audit record generation responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators; system developers.

Test: Automated mechanisms implementing audit record generation capability.

(CA) SECURITY ASSESSMENT AND AUTHORIZATION

DFPS requires that an initial assessment of the security controls for key information systems is performed to determine if the controls are effective in their application, controls are monitored on an ongoing basis to ensure their continued effectiveness and information systems containing potential vulnerabilities due to deficiencies in their controls are documented and acknowledged by the DFPS CISO and/or DFPS Executive Leadership. DFPS also requires that plans of action are designed by the DFPS Office of Information Security to correct deficiencies and reduce (or eliminate) vulnerabilities. DFPS Office of Information Security will ensure these controls are implemented in a timeframe per the plans of action.

The Security Assessment and Authorization control family includes controls that supplement the execution of security assessments, authorizations, continuous monitoring, plan of actions and milestones, and system interconnections. The intended audience for this Control includes, but is not limited to, the DFPS Chief Information Security Officer (CISO) and/or their designee and the Office of Information Security.

CA-01: SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Develops, documents, and disseminates to applicable personnel:
   1. Organization-level assessment, authorization, and monitoring policy that:
      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls;

b. Designate a senior management official as defined in the assessment, authorization, and monitoring policy to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures; and

c. Review and update the current assessment, authorization, and monitoring:
   1. Policy every year and following major changes to legislation or security requirements; and
   2. Procedures every year and following major changes to legislation or security requirements.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS must establish a security assessment procedure. [Source: DIR Control Standards Catalog CA-1]

Std.02 — The DFPS Information Security Officer shall be responsible for:

a. Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks;

b. Providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities under 1 TAC 202; and

c. Developing and recommending policies and establishing procedures and practices, in cooperation with the agency Information Resources Manager, information-owners and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, or disclosure. [Source: 1 TAC 202.21(b)(3, 5, 8)]

Std.03 — All information resources introduced into the Agency must be assessed by a qualified security assessor or an information security staff member, and authorized by the chief information security officer, prior to procurement (if commercially obtained) or implementation in a production environment (if internally developed). This requirement applies to all information resources regardless of ownership, custodianship, or usage.

SUPPLEMENTAL GUIDANCE

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Information Risk Management Policy. **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP 800-12, 800-30, 800-37, 800-39, 800-53A, 800-100, 800-137, 800- 137A; NIST IR 8062; FBI CJIS CSP v5.9	PM-9, PS-8, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Assessment, authorization, and monitoring policy and procedures; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with assessment, authorization, and monitoring policy responsibilities; organizational personnel with information security and privacy responsibilities.

CA-02: SECURITY ASSESSMENTS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;
b. Develop a control assessment plan that describes the scope of the assessment including:
   1. Controls and control enhancements under assessment;

2. Assessment procedures to be used to determine control effectiveness; and
3. Assessment environment, assessment team, and assessment roles and responsibilities;

c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;
d. Assess the controls in the system and its environment of operation at the frequency specified in Std.02 to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;
e. Produce a control assessment report that document the results of the assessment; and
f. Provide the results of the control assessment to personnel as identified in the assessment, authorization, and monitoring policy.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — A review of the DFPS information security program for compliance with these standards will be performed at least annually, based on business risk management decisions, by individual(s) independent of the information security program and designated by the DFPS Commissioner or their designated representative(s). [Source: DIR Control Standards Catalog CA-2]

Std.02 —

a. At least once every two years, DFPS must conduct an information security assessment of the agency's information resources systems, network systems, digital data storage systems, digital data security measures, and information resources vulnerabilities.
b. Not later than December 1 of the year in which DFPS conducts the assessment under Subsection (a), the agency shall report the results of the assessment to the Department of Information Resources, the governor, the lieutenant governor, and the speaker of the house of representatives.
c. DIR by rule may establish the requirements for the information security assessment and report required by this section. [Source: TX Govt. Code 2054.515]

Std.03 — Risk assessments conducted by Information Owners (or delegates) may take the place of control assessments if the system does not meet any of the following criteria:

a. High baseline;
b. Regulated Data; or
c. Confidential Internet-Facing system.

Std.04 — Systems may, at the direction of the DFPS CISO (or their delegate), be required to undergo a targeted or full security assessment.

SUPPLEMENTAL GUIDANCE

Organizations ensure that control assessors possess the required skills and technical expertise to develop effective assessment plans and to conduct assessments of system- specific, hybrid, common, and program management controls, as appropriate. The required skills include general knowledge of risk management concepts and approaches as well as comprehensive knowledge of and experience with the hardware, software, and firmware system components implemented.

Organizations assess controls in systems and the environments in which those systems operate as part of initial and ongoing authorizations, continuous monitoring, FISMA annual assessments, system design and development, systems security engineering, privacy engineering, and the system development life cycle. Assessments help to ensure that organizations meet information security and privacy requirements, identify weaknesses and deficiencies in the system design and development process, provide essential information needed to make risk-based decisions as part of authorization processes, and comply with vulnerability mitigation procedures. Organizations conduct assessments on the implemented controls as documented in security and privacy plans. Assessments can also be conducted throughout the system development life cycle as part of systems engineering and systems security engineering processes. The design for controls can be assessed as RFPs are developed, responses assessed, and design reviews conducted. If a design to implement controls and subsequent implementation in accordance with the design are assessed during development, the final control

testing can be a simple confirmation utilizing previously completed control assessment and aggregating the outcomes.

Organizations may develop a single, consolidated security and privacy assessment plan for the system or maintain separate plans. A consolidated assessment plan clearly delineates the roles and responsibilities for control assessment. If multiple organizations participate in assessing a system, a coordinated approach can reduce redundancies and associated costs.

Organizations can use other types of assessment activities, such as vulnerability scanning and system monitoring, to maintain the security and privacy posture of systems during the system life cycle. Assessment reports document assessment results in sufficient detail, as deemed necessary by organizations, to determine the accuracy and completeness of the reports and whether the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting requirements. Assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted. For example, assessments conducted in support of authorization decisions are provided to authorizing officials, senior agency officials for privacy, senior agency information security officers, and authorizing official designated representatives.

To satisfy annual assessment requirements, organizations can use assessment results from the following sources: initial or ongoing system authorizations, continuous monitoring, systems engineering processes, or system development life cycle activities. Organizations ensure that assessment results are current, relevant to the determination of control effectiveness, and obtained with the appropriate level of assessor independence. Existing control assessment results can be reused to the extent that the results are still valid and can also be supplemented with additional assessments as needed. After the initial authorizations, organizations assess controls during continuous monitoring. Organizations also establish the frequency for ongoing assessments in accordance with organizational continuous monitoring strategies. External audits, including audits by external entities such as regulatory agencies, are outside of the scope of CA-02.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Information Risk Management Policy; DFPS Security Control Assessment Plan. **State:** DIR Security Control Standards Catalog. **Federal:** OMB A-130; NIST SP 800-12, 800-30, 800-37, 800-39, 800-53A, 800-100, 800-137, 800- 137A; NIST IR 8062; FBI CJIS CSP v5.9	AC-20, CA-5, CA-6, CA-7, PM-9, RA-5, RA-10, SA-11, SC-38, SI-3, SI-12, SR-2, SR-3.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Assessment, authorization, and monitoring policy; procedures addressing assessment planning; procedures addressing control assessments; control assessment plan; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with control assessment responsibilities; organizational personnel with information security and privacy responsibilities.

Test: Automated mechanisms supporting control assessment, control assessment plan development, and/or control assessment reporting.

CA-02(01): INDEPENDENT ASSESSORS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization employs assessors or assessment teams with no operational responsibilities for the information system being assessed to conduct security control assessments.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Only high-rated systems, moderate-rated systems with Confidential data, and moderate-rated systems with Confidential data that are also Internet facing, must have a control assessment conducted by an independent assessor or assessment team, unless otherwise directed by the DFPS CISO.

SUPPLEMENTAL GUIDANCE

Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of systems. Impartiality means that assessors are free from any perceived or actual conflicts of interest regarding the development, operation, sustainment, or management of the systems under assessment or the determination of control effectiveness. To achieve impartiality, assessors do not create a mutual or conflicting interest with the organizations where the assessments are being conducted, assess their own work, act as management or employees of the organizations they are serving, or place themselves in positions of advocacy for the organizations acquiring their services.

Independent assessments can be obtained from elements within organizations or be contracted to public or private sector entities outside of organizations. Authorizing officials determine the required level of independence based on the security categories of systems and/or the risk to organizational operations, organizational assets, or individuals.

Authorizing officials also determine if the level of assessor independence provides sufficient assurance that the results are sound and can be used to make credible, risk-based decisions. Assessor independence determination includes whether contracted assessment services have sufficient independence, such as when system owners are not directly involved in contracting processes or cannot influence the impartiality of the assessors conducting the assessments. During the system design and development phase, having independent assessors is analogous to having independent SMEs involved in design reviews.

When organizations that own the systems are small or the structures of the organizations require that assessments be conducted by individuals that are in the developmental, operational, or management chain of the system owners, independence in assessment processes can be achieved by ensuring that assessment results are carefully reviewed and analyzed by independent teams of experts to validate the completeness, accuracy, integrity, and reliability of the results. Assessments performed for purposes other than to support authorization decisions are more likely to be useable for such decisions when performed by assessors with sufficient independence, thereby reducing the need to repeat assessments.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Information Risk Management Policy; DFPS Security Control Assessment Plan. **State:** DIR Security Control Standards Catalog. **Federal:** OMB A-130; NIST SP 800-12, 800-30, 800-37, 800-39, 800-53A, 800-100, 800-137, 800- 137A; NIST IR 8062; FBI CJIS CSP v5.9	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Organizational personnel with control assessment responsibilities; organizational personnel with information security and privacy responsibilities.

Interview: Automated mechanisms supporting control assessment.

CA-03: SYSTEM INTERCONNECTIONS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Approve and manage the exchange of information between the system and other systems using interconnection security agreements (ISAs);
b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and
c. Review and update the agreements annually.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Authorize connections from the internal/organization information system to other information systems outside of DFPS through the use of Interconnection Security Agreements (ISA) or other comparable agreements (such as MOU/MOA, SLA, or specific contractual clause, so long as the appropriate interconnection detail is provided therein) and monitor/control the system connections on an ongoing basis. [Source: DIR Control Standards Catalog CA-3]

Std.02 — All ISAs must be approved by the DFPS Chief Information Security Officer.

Std.03 — Reviews and updates the interconnection agreements on an ongoing basis, no less often than once every year and whenever significant changes (that can affect the security state of the information system) are implemented that could impact the validity of the agreement as a verification of enforcement of security requirements.

SUPPLEMENTAL GUIDANCE

System information exchange requirements apply to information exchanges between two or more systems. System information exchanges include connections via leased lines or virtual private networks, connections to internet service providers, database sharing or exchanges of database transaction information, connections and exchanges with cloud services, exchanges via web-based services, or exchanges of files via file transfer protocols, network protocols (e.g., IPv4, IPv6), email, or other organization-to-organization communications.

Organizations consider the risk related to new or increased threats that may be introduced when systems exchange information with other systems that may have different security and privacy requirements and controls. This includes systems within the same organization and systems that are external to the organization. A joint authorization of the systems exchanging information may help to communicate and reduce risk.

Authorizing officials determine the risk associated with system information exchange and the controls needed for appropriate risk mitigation. The types of agreements selected are based on factors such as the impact level of the information being exchanged, the relationship between the organizations exchanging information (e.g., government to government, government to business, business to business, government or business to service provider, government or business to individual), or the level of access to the organizational system by users of the other system. If systems that exchange information have the same authorizing official, organizations need not develop agreements. Instead, the interface characteristics between the systems (e.g., how the information is being exchanged. how the information is protected) are described in the respective security and privacy plans. If the systems that exchange information have different authorizing officials within the same organization, the

organizations can develop agreements or provide the same information that would be provided in the appropriate agreement type from CA-03a in the respective security and privacy plans for the systems. Organizations may incorporate agreement information into formal contracts, especially for information exchanges established between federal agencies and nonfederal organizations (including service providers, contractors, system developers, and system integrators). Risk considerations include systems that share the same networks

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Information Risk Management Policy; DFPS Security Control Assessment Plan. **State:** DIR Security Control Standards Catalog. **Federal:** OMB A-130; FIPS 199; NIST SP 800-47; FBI CJIS CSP v5.9	AC-4, AC-20, AU-16, CA-6, IA-3, IR-4, PL-2, PT-7, RA-3, SA-9, SC-7, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing system connections; system and communications protection policy; system interconnection security agreements; information exchange security agreements; memoranda of understanding or agreements; service level agreements; non-disclosure agreements; system design documentation; system configuration settings and associated documentation; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with responsibilities for developing, implementing, or approving system interconnection agreements; organizational personnel with information security and privacy responsibilities; personnel managing the system(s) to which the interconnection security agreement applies.

CA-05: PLAN OF ACTION AND MILESTONES

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and

b. Update existing plan of action and milestones as corrective actions occur, and review at least quarterly until all findings are resolved, based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Develop and update a plan of action and milestones for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system. [Source: DIR Control Standards Catalog CA-5]

Std.02 — An agency-wide information security program must be approved by the agency head and include a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency. [Source: 1 TAC 202.24(a)(5)].

SUPPLEMENTAL GUIDANCE

Plans of action and milestones are useful for any type of organization to track planned remedial actions. Plans of action and milestones are required in authorization packages and subject to federal reporting requirements established by OMB.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Information Risk Management Policy; DFPS Security Control Assessment Plan. **State:** 1 TAC 202.24(a)(5); DIR Security Control Standards Catalog **Federal:** OMB A-130; NIST SP 800-37; FBI CJIS CSP v5.9	CA-2, CA-7, PM-4, PM-9, RA-7, SI-2, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Assessment, authorization, and monitoring policy; procedures addressing plan of action and milestones; control assessment plan; control assessment report; control assessment evidence; plan of action and milestones; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with plan of action and milestones development and implementation responsibilities; organizational personnel with information security and privacy responsibilities.

Test: Automated mechanisms for developing, implementing, and maintaining plan of action and milestones.

CA-06: AUTHORIZATION

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Assign a senior official as the authorizing official for the system;
b. Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems;
c. Ensure that the authorizing official for the system, before commencing operations:
   1. Accepts the use of common controls inherited by the system; and

2. Authorizes the system to operate;

d. Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems;
e. Update the authorizations per Stds.05 & 06.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Authorize the information system for processing before operations or when there is a significant change to the system. [Source: DIR Control Standards Catalog CA-6]

Std.02 — A senior organization official must sign and approve the security accreditation. [Source: DIR Control Standards Catalog CA-6]

Std.03 — The DFPS Commissioner or his/her designated representative(s) must approve high level risk management decisions as required by 1 TAC 202. [Source: 1 TAC 202.20(6)]

Std.04 — Approval of the security risk acceptance, transference, or mitigation decision shall be the responsibility of the DFPS Chief Information Security Officer or their designee(s), in coordination with the information owner, for systems identified with a Low or Moderate residual risk; and the DFPS Commissioner for all systems identified with a residual High Risk. [Source: 1 TAC 202.25(4)]

Std.05 — The security authorization for a system is updated:

a. When significant changes are made to the system;
b. When changes in requirements result in a different security baseline;
c. When changes occur to authorizing legislation, regulatory standards, or federal requirements that impact the system;
d. After the occurrence of a serious security violation which raises questions about the validity of an earlier security authorization; or
e. Three years after the last authorization.

Std.06 — The security authorization for common controls is updated:

a. When changes occur to authorizing legislation, organization policy, regulatory standards, or federal requirements that affect the controls;
b. After the occurrence of a serious security violation which raises questions about the validity of an earlier security authorization; or
c. Three years after the last authorization.

Std.07 — Assessments, authorizations, and decisions may be included in the accreditation package in accordance with the DFPS Authority to Operate Standard.

SUPPLEMENTAL GUIDANCE

Authorizations are official management decisions by senior officials to authorize operation of systems, authorize the use of common controls for inheritance by organizational systems, and explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of agreed-upon controls.

Authorizing officials provide budgetary oversight for organizational systems and common controls or assume responsibility for the mission and business functions supported by those systems or common controls. The authorization process is a federal responsibility, and therefore, authorizing officials must be federal employees. Authorizing officials are both responsible and accountable for security and privacy risks associated with the operation and use of organizational systems. Nonfederal organizations may have similar processes to authorize systems and senior officials that assume the authorization role and associated responsibilities.

Authorizing officials issue ongoing authorizations of systems based on evidence produced from implemented continuous monitoring programs. Robust continuous monitoring programs reduce the need for separate reauthorization processes. Through the employment of comprehensive continuous monitoring processes, the

information contained in authorization packages (i.e., security and privacy plans, assessment reports, and plans of action and milestones) is updated on an ongoing basis. This provides authorizing officials, common control providers, and system owners with an up-to-date status of the security and privacy posture of their systems, controls, and operating environments. To reduce the cost of reauthorization, authorizing officials can leverage the results of continuous monitoring processes to the maximum extent possible as the basis for rendering reauthorization decisions.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Information Risk Management Policy; DFPS Security Control Assessment Plan. **State:** 1 TAC 202.20(6), TAC 202.25(4); DIR Security Control Standards Catalog **Federal:** OMB A-130; NIST SP 800-37, 800-137; FBI CJIS CSP v5.9	CA-2, CA-3, CA-7, PM-9, PM-10, RA-3, SA-10, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Assessment, authorization, and monitoring policy; procedures addressing authorization; system security plan, privacy plan, assessment report, plan of action and milestones; authorization statement; other relevant documents or records.

Interview: Organizational personnel with authorization responsibilities; organizational personnel with information security and privacy responsibilities.

Test: Automated mechanisms that facilitate authorizations and updates.

CA-07: CONTINUOUS MONITORING

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization develops a system-level continuous monitoring strategy and implements continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:

a. Establishing the following system-level metrics to be monitored: metrics defined in the Continuous Monitoring Program;
b. Establishing frequencies as specified in the Continuous Monitoring Program for monitoring and frequencies as specified in the risk management program policy for assessment of control effectiveness;
c. Ongoing control assessments in accordance with the continuous monitoring strategy;
d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy
e. Correlation and analysis of information generated by control assessments and monitoring;
f. Response actions to address results of the analysis of control assessment and monitoring information; and
g. Reporting the security and privacy status of the system to the personnel and at the frequencies specified in Stds.02 & 03.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Monitor the security controls in the information system on an ongoing basis. [Source: DIR Control Standards Catalog CA-7]

Std.02 — The DFPS Chief Information Security Officer is responsible for reporting, at least annually, to the DFPS Commissioner the status and effectiveness of security controls. [Source: 1 TAC 202.21(b)(11)]

Std.03 — The DFPS Information Security Officer must report, at least annually, to the DFPS Commissioner on the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the requirements of 1 TAC 202 and the effectiveness of current information security program and status of key initiatives. [Source: 1 TAC 202.23(a)(1)]

SUPPLEMENTAL GUIDANCE

Continuous monitoring at the system level facilitates ongoing awareness of the system security and privacy posture to support organizational risk management decisions. The terms "continuous" and "ongoing" imply that organizations assess and monitor their controls and risks at a frequency sufficient to support risk-based decisions. Different types of controls may require different monitoring frequencies. The results of continuous monitoring generate risk response actions by organizations. When monitoring the effectiveness of multiple controls that have been grouped into capabilities, a root-cause analysis may be needed to determine the specific control that has failed. Continuous monitoring programs allow organizations to maintain the authorizations of systems and common controls in highly dynamic environments of operation with changing mission and business needs, threats, vulnerabilities, and technologies. Having access to security and privacy information on a continuing basis through reports and dashboards gives organizational officials the ability to make effective and timely risk management decisions, including ongoing authorization decisions.

Automation supports more frequent updates to hardware, software, and firmware inventories, authorization packages, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Continuous monitoring activities are scaled in accordance with the security categories of systems. Monitoring requirements, including the need for specific monitoring, may be referenced in other controls and control enhancements, such as AC-02g, AC-17(01), AT-04a, CM-03f, CM-06d, CM-11c, IR-05, MA- 02b, MA-03a, MA-04a, PE-03d, PE-06, PE-14b, PE-16, PM-06, PM-31, PS-07e, SA-09c, SC-07a, SC-07(24)(b), SC-18b, SI-04, and SR-04.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Information Risk Management Policy; DFPS Security Control Assessment Plan. **State:** 1 TAC 202.21(b)(11), 1 TAC 202.23(a), 1 TAC 202.23(a)(1); DIR Security Control Standards Catalog. **Federal:** OMB A-130; NIST SP 800-37, 800-39, 800-53A, 800-115, 800-137; NIST IR 8011-1, 8062; FBI CJIS CSP v5.9	AC-2, AC-6, AC-17, AT-4, AU-6, AU-13, CA-2, CA-5, CA-6, CM-3, CM-4, CM-6, CM-11, IA-5, IR-5, MA-2, MA-3, MA-4, PE-3, PE-6, PE-14, PE-16, PE-20, PL-2, PM-4, PM-6, PM-9, PM-10, PM-12, PM-14, PM-23, PM-28, PM-31, PS-7, PT-7, RA-3, RA-5, RA-7, RA-10, SA-8, SA-9, SA-11, SC-5, SC-7, SC-18, SC-38, SC-43, SI-3, SI-4, SI-12, SR-6.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Assessment, authorization, and monitoring policy; organizational continuous monitoring strategy; system-level continuous monitoring strategy; procedures addressing continuous monitoring of system controls; procedures addressing configuration management; control assessment report; plan of action and milestones;

system monitoring records; configuration management records; impact analyses; status reports; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with continuous monitoring responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators.

Test: Mechanisms implementing continuous monitoring; mechanisms supporting response actions to address assessment and monitoring results; mechanisms supporting security and privacy status reporting.

CA-07(01): INDEPENDENT ASSESSMENT

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization employs independent assessors or assessment teams to monitor the controls in the system on an ongoing basis.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Employ assessors at the DFPS CISO-defined level of independence in accordance with CA-02 and CA-02(01).

SUPPLEMENTAL GUIDANCE

Organizations maximize the value of control assessments by requiring that assessments be conducted by assessors with appropriate levels of independence. The level of required independence is based on organizational continuous monitoring strategies. Assessor independence provides a degree of impartiality to the monitoring process. To achieve such impartiality, assessors do not create a mutual or conflicting interest with the organizations where the assessments are being conducted, assess their own work, act as management or employees of the organizations they are serving, or place themselves in advocacy positions for the organizations acquiring their services.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Information Risk Management Policy; DFPS Security Control Assessment Plan. **State:** DIR Security Control Standards Catalog. **Federal:** OMB A-130; NIST SP 800-37, 800-39, 800-53A, 800-115, 800-137; NIST IR 8011-1, 8062; FBI CJIS CSP v5.9	AC-2, AC-6, AC-17, AT-4, AU-6, AU-13, CA-2, CA-5, CA-6, CM-3, CM-4, CM-6, CM-11, IA-5, IR-5, MA-2, MA-3, MA-4, PE-3, PE-6, PE-14, PE-16, PE-20, PL-2, PM-4, PM-6, PM-9, PM-10, PM-12, PM-14, PM-23, PM-28, PM-31, PS-7, PT-7, RA-3, RA-5, RA-7, RA-10, SA-8, SA-9, SA-11, SC-5, SC-7, SC-18, SC-38, SC-43, SI-3, SI-4, SI-12, SR-6.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Assessment, authorization, and monitoring policy; organizational continuous monitoring strategy; system-level continuous monitoring strategy; procedures addressing continuous monitoring of system controls;

control assessment report; plan of action and milestones; system monitoring records; impact analyses; status reports; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with continuous monitoring responsibilities; organizational personnel with information security and privacy responsibilities

CA-08: PENETRATION TESTING

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization conducts penetration testing at the frequency identified in Std.02 on assets as identified in Std.03 that create, access, process, transmit, or store any DFPS information classified as Confidential or Controlled.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS, as a state agency implementing an Internet website or mobile application that processes any sensitive personal or personally identifiable information or confidential information must:

a. Submit a biennial data security plan to the Department of Information Resources not later than October 15 of each even-numbered year to establish planned beta testing for the website or application; and
b. Subject the website or application to a vulnerability and penetration test and address any vulnerability identified in the test. [Source: TX Govt. Code 2054.516(a)(2)]

Std.02 — Penetration Test Frequency

a. Internet websites and mobile application penetration tests:
    1. Prior to an authority to operate being granted for the system to go into production.
    2. Whenever there is a major system change.
b. DFPS performs external facing penetration test at least annually.

Std.03 — Penetration Test Types

a. Internet websites and mobile application penetration tests: Conduct a penetration test that includes both credentialed and non-credentialed dynamic application security testing
b. Organization performs external-facing penetration test: Conduct a penetration test that includes:
    1. Coverage for the entire environment, perimeter, and critical systems;
    2. Reviewing and considering threats and vulnerabilities experienced in the last 12 months;

Std.04 — All identified vulnerabilities must be documented in the organization's risk register.

SUPPLEMENTAL GUIDANCE

Penetration testing is a specialized type of assessment conducted on systems or individual system components to identify vulnerabilities that could be exploited by adversaries.

Penetration testing goes beyond automated vulnerability scanning and is conducted by agents and teams with demonstrable skills and experience that include technical expertise in network, operating system, and/or application level security. Penetration testing can be used to validate vulnerabilities or determine the degree of penetration resistance of systems to adversaries within specified constraints. Such constraints include time, resources, and skills. Penetration testing attempts to duplicate the actions of adversaries and provides a more in-depth analysis of security- and privacy-related weaknesses or deficiencies.

Penetration testing is especially important when organizations are transitioning from older technologies to newer technologies (e.g., transitioning from IPv4 to IPv6 network protocols).

Organizations can use the results of vulnerability analyses to support penetration testing activities. Penetration testing can be conducted internally or externally on the hardware, software, or firmware components of a system and can exercise both physical and technical controls. A standard method for penetration testing includes a pretest analysis based on full knowledge of the system, pretest identification of potential vulnerabilities based on the pretest analysis, and testing designed to determine the exploitability of vulnerabilities. All parties agree to the rules of engagement before commencing penetration testing scenarios. Organizations correlate the rules of engagement for the penetration tests with the tools, techniques, and procedures that are anticipated to be employed by adversaries. Penetration testing may result in the exposure of information that is protected by laws or regulations, to individuals conducting the testing. Rules of engagement, contracts, or other appropriate mechanisms can be used to communicate expectations for how to protect this information. Risk assessments guide the decisions on the level of independence required for the personnel conducting penetration testing.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Information Risk Management Policy; DFPS Security Control Assessment Plan; DFPS Vulnerability Management policy. **State:** TX Govt. Code 2054.516; DIR Security Control Standards Catalog. **Federal:** FBI CJIS CSP v5.9	RA-5, RA-10, SA-11, SR-5, SR-6.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Assessment, authorization, and monitoring policy; procedures addressing penetration testing; assessment plan; penetration test report; assessment report; assessment evidence; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with control assessment responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators.

Test: Automated mechanisms supporting penetration testing.

CA-08(01): INDEPENDENT PENETRATION AGENT OR TEAM

Priority: P1

Baseline(s): High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization employs an independent penetration agent or penetration team to perform penetration testing on the information system or system components.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — The independent penetration agent or penetration team must be a DFPS CISO approved independent penetration test vendor.

SUPPLEMENTAL GUIDANCE	
Independent penetration agents or teams are individuals or groups who conduct impartial penetration testing of organizational information systems. Impartiality implies that penetration agents or teams are free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the information systems that are the targets of the penetration testing. Supplemental guidance for CA-2 (1) provides additional information regarding independent assessments that can be applied to penetration testing.	
REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Information Risk Management Policy; DFPS Security Control Assessment Plan; DFPS Vulnerability Management policy. **State:** TX Govt. Code 2054.516; DIR Security Control Standards Catalog. **Federal:** FBI CJIS CSP v5.9	CA-2.
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Assessment, authorization, and monitoring policy; procedures addressing penetration testing; assessment plan; penetration test report; assessment report; security assessment evidence; system security plan; privacy plan; other relevant documents or records. Interview: Organizational personnel with assessment responsibilities; organizational personnel with information security and privacy responsibilities.	

CA-09: INTERNAL SYSTEM CONNECTIONS	
Priority: P1	
Baseline(s): High	Overlay(s): DIR, CJIS
CONTROL REQUIREMENTS	
The organization: a. Authorize internal connections of all system components or classes of components defined in the applicable System Security Plan (SSP) to the system; b. Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated; c. Terminate internal system connections after session limits specified in the System Security Plan (SSP); and d. Review at the frequency specified in the Continuous Monitoring Program, or at least annually if not otherwise specified, the continued need for each internal connection.	
AGENCY IMPLEMENTATION STANDARDS	
Std.01 — DFPS must have a procedure for authorizing internal information resource connections. [Source: DIR Control Standards Catalog CA-9]	

Std.02 — For any system categorized as moderate or high, the System Security Plan (SSP) will identify the types of personally owned equipment that may be internally connected with organizational information systems and networks, compliant with DFPS mobile device security policies.

SUPPLEMENTAL GUIDANCE

Internal system connections are connections between organizational systems and separate constituent system components (i.e., connections between components that are part of the same system) including components used for system development. Intra-system connections include connections with mobile devices, notebook and desktop computers, tablets, printers, copiers, facsimile machines, scanners, sensors, and servers. Instead of authorizing each internal system connection individually, organizations can authorize internal connections for a class of system components with common characteristics and/or configurations, including printers, scanners, and copiers with a specified processing, transmission, and storage capability or smart phones and tablets with a specific baseline configuration. The continued need for an internal system connection is reviewed from the perspective of whether it provides support for organizational missions or business functions.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Security Control Assessment Plan. **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP 800-124; NIST IR 8023; FBI CJIS CSP v5.9	AC-3, AC-4, AC-18, AC-19, CM-2, IA-3, SC-7, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Assessment, authorization, and monitoring policy; procedures addressing penetration testing; assessment plan; penetration test report; assessment report; security assessment evidence; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with assessment responsibilities; organizational personnel with information security and privacy responsibilities.

Test: Mechanisms supporting internal system connections.

(CM) CONFIGURATION MANAGEMENT

DFPS establishes and maintains baseline configurations and inventories of DFPS information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. DFPS also establishes and enforces security configuration settings for information technology products employed in DFPS information systems.

The intended audience for this Control includes, but is not limited to, information resource owners and custodians. Information resource owner, or designee, is responsible for ensuring that the configuration management measures described in this Control family are implemented by personnel with configuration management responsibilities (e.g. system/network administrators, information security analyst, etc.).

CM-01: CONFIGURATION MANAGEMENT POLICY AND PROCEDURES

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Develop, document, and disseminate to appropriate personnel:
   1. Organization-level configuration management policy that:
      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls;
b. Designate a senior management official as defined in the configuration management policy to manage the development, documentation, and dissemination of the configuration management policy and procedures; and
c. Review and update the current configuration management:
   1. Policy every year and following major changes to legislation or security requirements; and
   2. Procedures every year and following major changes to legislation or security requirements.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Establish the process for controlling modifications to hardware, software, firmware, and documentation to ensure the information resources are protected against improper modification before, during, and after system implementation. [Source: DIR Control Standards Catalog CM-1]

Std.02 — The DFPS Information Security Officer shall be responsible for:

a. Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks;
b. Providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities under 1 TAC 202; and
c. Developing and recommending policies and establishing procedures and practices, in cooperation with the agency Information Resources Manager, information-owners and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, or disclosure. [Source: 1 TAC 202.21(b)(3, 5, 8)]

SUPPLEMENTAL GUIDANCE

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CM family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

REFERENCES	**RELATED CONTROLS**

Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** OMB A-130; NIST SP 800-12, 800-30, 800-39, 800-100; FBI CJIS CSP v5.9	PM-9, PS-8, SA-8, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy and procedures; security and privacy program policies and procedures; assessment or audit findings; documentation of security incidents or breaches; system security plan; privacy plan; risk management strategy; other relevant artifacts, documents, or records.

Interview: Organizational personnel with configuration management responsibilities; organizational personnel with information security and privacy responsibilities.

CM-02: BASELINE CONFIGURATION

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Develop, document, and maintain under configuration control, a current baseline configuration of the system; and
b. Review and update the baseline configuration of the system:
    1. Annually;
    2. When required due to a major system change; and
    3. When system components are installed or upgraded.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS must keep confidential its network security information according as detailed in its Information Security Monitoring Baseline Configuration Specifications. [Source: TX Govt. Code 2059.055(b)(1, 2, 3)]

Std.02 — Information Technology Services (ITS) assets must comply with the DFPS Configuration Management Policy.

SUPPLEMENTAL GUIDANCE

Baseline configurations for systems and system components include connectivity, operational, and communications aspects of systems. Baseline configurations are documented, formally reviewed, and agreed-upon specifications for systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, or changes to systems and include security and privacy control implementations, operational procedures, information about system components, network topology, and logical placement of components in the system architecture. Maintaining baseline configurations requires creating new

baselines as organizational systems change over time. Baseline configurations of systems reflect the current enterprise architecture.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Configuration Management Policy. **State:** TX Govt. Code 2059.055; DIR Security Control Standards Catalog. **Federal:** NIST SP 800-124, 800-128; FBI CJIS CSP v5.9	AC-19, AU-6, CA-9, CM-1, CM-3, CM-5, CM-6, CM-8, CM-9, CP-9, CP-10, CP-12, MA-2, PL-8, PM-5, SA-8, SA-10, SA-15, SC-18.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; procedures addressing the baseline configuration of the system; configuration management plan; enterprise architecture documentation; system design documentation; system security plan; privacy plan; system architecture and configuration documentation; system configuration settings and associated documentation; system component inventory; change control records; other relevant documents or records

Interview: Organizational personnel with configuration management responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators.

Test: Organizational processes for managing baseline configurations; automated mechanisms supporting configuration control of the baseline configuration.

CM-02(01): REVIEWS AND UPDATES

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

This control has been withdrawn and incorporated in CM-02. CM-02(1) is referenced in the FBI CJIS Security Policy. Please see CM-02 for these requirements.

CM-02(02): AUTOMATION SUPPORT FOR ACCURACY AND CURRENCY

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using automated mechanisms as defined in applicable System Security Plans (SSPs).

AGENCY IMPLEMENTATION STANDARDS
None.
SUPPLEMENTAL GUIDANCE
Automated mechanisms that help organizations maintain consistent baseline configurations for systems include configuration management tools, hardware, software, firmware inventory tools, and network management tools. Automated tools can be used at the organization level, mission and business process level, or system level on workstations, servers, notebook computers, network components, or mobile devices. Tools can be used to track version numbers on operating systems, applications, types of software installed, and current patch levels. Automation support for accuracy and currency can be satisfied by the implementation of CM-08(02) for organizations that combine system component inventory and baseline configuration activities.4

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP 800-124, 800-128; FBI CJIS CSP v5.9	CM-7, IA-3, RA-5.

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Configuration management policy; procedures addressing the baseline configuration of the system; configuration management plan; system architecture and configuration documentation; system configuration settings and associated documentation; copies of previous baseline configuration versions; system security plan; other relevant documents or records. Interview: Organizational personnel with configuration management responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators. Test: Organizational processes for managing baseline configurations.

CM-02(03): RETENTION OF PREVIOUS CONFIGURATIONS

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): DIR, CJIS
CONTROL REQUIREMENTS	
Retain at least the latest approved and a minimum of one previous versions of baseline configurations of the system to support rollback.	
AGENCY IMPLEMENTATION STANDARDS	

Std.01 — Storage must comply with CM-02.

Std.02 — Change control procedures must include back-out procedures.

SUPPLEMENTAL GUIDANCE

Retaining previous versions of baseline configurations to support rollback includes hardware, software, firmware, configuration files, configuration records, and associated documentation.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP 800-124, 800-128; FBI CJIS CSP v5.9	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; procedures addressing the baseline configuration of the system; configuration management plan; system architecture and configuration documentation; system configuration settings and associated documentation; copies of previous baseline configuration versions; system security plan; other relevant documents or records.

Interview: Organizational personnel with configuration management responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators.

Test: Organizational processes for managing baseline configurations.

CM-02(07): CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization:

a. Issue travel-configured information technology assets when Std.01 applies with FIPS 140-2 whole-disk encryption and mandatory remote access connection authorized per AC-17 to individuals traveling to locations that the organization deems to be of significant risk; and
b. Apply the following controls to the systems or components when the individuals return from travel: malware scanning and/or reimaging.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Applies to any information technology assets being transported to countries listed on the US Department of State's travel advisory website that has a level of advice "Level 2 – Exercise increased caution" or higher.

Std.02 — Before taking DFPS electronic devices outside of the USA or accessing the DFPS network while outside of the USA, DFPS staff must:

a. Submit an official request for access;
b. Receive explicit approval from the DFPS Chief Information Security Officer or their designee no less than 10 business days prior to departure.

Std.03 — If approval is granted, examine returned computers for signs of tampering:

a. If evidence exists, follow the implementation standards established in IR-06;
b. If evidence of tampering does not exist, follow standard operating procedures to have the equipment scanned for malware (and re-imaged for the next travelling user if using loaned equipment).

SUPPLEMENTAL GUIDANCE

When it is known that information systems, system components, or devices (e.g., notebook computers, mobile devices) will be located in high-risk areas, additional security controls may be implemented to counter the greater threat in such areas coupled with the lack of physical security relative to organizational-controlled areas. For example, organizational policies and procedures for notebook computers used by individuals departing on and returning from travel include, for example, determining which locations are of concern, defining required configurations for the devices, ensuring that the devices are configured as intended before travel is initiated, and applying specific safeguards to the device after travel is completed. Specially configured notebook computers include, for example, computers with sanitized hard drives, limited applications, and additional hardening (e.g., more stringent configuration settings). Specified safeguards applied to mobile devices upon return from travel include, for example, examining the device for signs of physical tampering and purging/reimaging the hard disk drive. Protecting information residing on mobile devices is covered in the media protection family.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Information Security While Traveling Abroad. **State:** TX Govt. Code 2059.055; DIR Security Control Standards Catalog. **Federal:** NIST SP 800-124, 800-128; FBI CJIS CSP v5.9	MP-4, MP-5.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the system; procedures addressing system component installations and upgrades; system architecture and configuration documentation; system configuration settings and associated documentation; system component inventory; records of system baseline configuration reviews and updates;

system component installations/upgrades and associated records; change control records; system security plan; other relevant documents or records.

Interview: Organizational personnel with configuration management responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators.

Test: Organizational processes for managing baseline configurations.

CM-03: CONFIGURATION CHANGE CONTROL

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Determine and document the types of changes to the system that are configuration-controlled;
b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;
c. Document configuration change decisions associated with the system;
d. Implement approved configuration-controlled changes to the system;
e. Retain records of configuration-controlled changes to the system for at least one change cycles of baseline configurations as defined in CM-02(03), and as feasible for the life of the system;
f. Monitor and review activities associated with configuration-controlled changes to the system; and
g. Coordinate and provide oversight for configuration change control activities through the Change Approval Board (CAB) that convenes per agency change control procedures and when there is a significant change to systems or environments.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — The DFPS system owner coordinates and provides oversight for configuration change control activities through the DFPS configuration change control element (e.g. DFPS Change Approval Board (CAB)) that convenes according to organization-defined frequency and according to organization-defined configuration change conditions.

Std.02 — Any change affecting the computing environment (HVAC, water, plumbing, alarms, etc.) must be coordinated with the appropriate IT staff to ensure compliance with the change management process.

Std.03 - All changes must be auditable and audited.

SUPPLEMENTAL GUIDANCE

Configuration change control for organizational systems involves the systematic proposal, justification, implementation, testing, review, and disposition of system changes, including system upgrades and modifications. Configuration change control includes changes to baseline configurations, configuration items of systems, operational procedures, configuration settings for system components, remediate vulnerabilities, and unscheduled or unauthorized changes. Processes for managing configuration changes to systems include Configuration Control Boards or Change Advisory Boards that review and approve proposed changes. For changes that impact privacy risk, the senior agency official for privacy updates privacy impact assessments and system of records notices. For new systems or major upgrades, organizations consider including representatives from the development organizations on the Configuration Control Boards or Change Advisory Boards. Auditing of changes includes activities before and after changes are made to systems and the auditing activities required to implement such changes. See also SA-10.

The configuration change control process for the information system, system components, or changes to the configuration settings for information technology products (including, but not limited to, operating systems, applications, firewalls, and routers) should include a systematic proposal, justification, implementation,

test/evaluation, review, and disposition of changes to the information system, including upgrades and modifications.

Normal and emergency changes, including changes resulting from the remediation of flaws, should be included in the configuration change control process. All changes should be tested, validated, and documented before implementation on operational systems.

Testing should not interfere with normal operations. An operational system may need to be taken off-line, or replicated to the extent feasible, before testing can be conducted. If an information system must be taken off-line for testing, the tests should be scheduled to occur during planned system outages whenever possible. In situations where the operational system cannot be tested without disrupting mission-critical functions, employ compensating controls (for example, providing a replicated system to conduct testing) in accordance with the general tailoring guidance.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** TX Govt. Code 2059.055; DIR Security Control Standards Catalog. **Federal:** NIST SP 800-124, 800-128; NIST IR 8062; FBI CJIS CSP v5.9	CA-7, CM-2, CM-4, CM-5, CM-6, CM-9, CM-11, IA-3, MA-2, PE-16, PT-6, RA-8, SA-8, SA-10, SC-28, SC-34, SC-37, SI-2, SI-3, SI-4, SI-7, SI-10, SR-11.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; procedures addressing system configuration change control; configuration management plan; system architecture and configuration documentation; change control records; system audit records; change control audit and review reports; agenda/minutes/documentation from configuration change control oversight meetings; system security plan; privacy plan; privacy impact assessments; system of records notices; other relevant documents or records.

Interview: Organizational personnel with configuration change control responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators; members of change control board or similar.

Test: Organizational processes for configuration change control; automated mechanisms that implement configuration change control.

CM-03(01): AUTOMATED DOCUMENT / NOTIFICATION / PROHIBITION OF CHANGES

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

For systems processing CJIS data, the following additional Implementation Standard applies:

The organization employs automated mechanisms to:

a. Document proposed changes to the information system;

b. Notify designated approval authorities (defined in the SSP) of proposed changes to the information system;
c. Request change approval per the system configuration management documentation;
d. Highlight proposed changes that have been waiting an approval decision, or have not been approved, for longer than change management procedure (defined in the SSP) requires;
e. Prohibit changes to the information system until approvals are received;
f. Document all changes to the information system; and
g. Notify stakeholders when approved changes are completed.

The list of potential stakeholders must include, but is not limited to the following:

a. Change Control Board (CCB);
b. Configuration Management Executive;
c. Chief Information Security Officer (CISO)
d. Program Manager;
e. Data Guardian;
f. Information System Owner; and
g. Information System Administrator

AGENCY IMPLEMENTATION STANDARDS

Std.01 - This control requirements applies to DFPS systems processing CJIS data.

SUPPLEMENTAL GUIDANCE

N/A

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP 800-124, 800-128; NIST IR 8062; FBI CJIS CSP v5.9	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; procedures addressing system configuration change control; configuration management plan; system design documentation; system architecture and configuration documentation; automated configuration control mechanisms; system configuration settings and associated documentation; change control records; system audit records; change approval requests; change approvals; system security plan; other relevant documents or records.

Interview: Organizational personnel with configuration change control responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers; members of change control board or similar.

Test: Organizational processes for configuration change control; automated mechanisms implementing configuration change control activities.

CM-03(02): TEST / VALIDATE / DOCUMENT CHANGES

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization test, validate, and document changes to the system before finalizing the implementation of the changes.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Change control procedures must include functionality testing to verify that the change does not adversely impact the security of the system.

SUPPLEMENTAL GUIDANCE

Changes to systems include modifications to hardware, software, or firmware components and configuration settings defined in CM-06. Organizations ensure that testing does not interfere with system operations that support organizational mission and business functions. Individuals or groups conducting tests understand security and privacy policies and procedures, system security and privacy policies and procedures, and the health, safety, and environmental risks associated with specific facilities or processes. Operational systems may need to be taken offline, or replicated to the extent feasible, before testing can be conducted. If systems must be taken offline for testing, the tests are scheduled to occur during planned system outages whenever possible. If the testing cannot be conducted on operational systems, organizations employ compensating controls.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS IRM CAB Charter. **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP 800-124, 800-128; NIST IR 8062; FBI CJIS CSP v5.9	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; configuration management plan; procedures addressing system configuration change control; system design documentation; system architecture and configuration documentation; system configuration settings and associated documentation; test records; validation records; change control records; system audit records; system security plan; other relevant documents or records.

Interview: Organizational personnel with configuration change control responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers; members of change control board or similar.

Test: Organizational processes for configuration change control; automated mechanisms supporting and/or implementing, testing, validating, and documenting system changes.

CM-03(04): SECURITY AND PRIVACY REPRESENTATIVE

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization requires information security and privacy representatives as designated by the CISO to be members of the configuration change control element defined in CM-03g.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — The DFPS Chief Information Security Officer or their delegate provides information security and privacy oversight for configuration change control activities through the Change Advisory Board (CAB).

SUPPLEMENTAL GUIDANCE

Information security representatives can include, for example, senior agency information security officers, information system security officers, or information system security managers. Representation by personnel with information security expertise is important because changes to information system configurations can have unintended side effects, some of which may be security relevant. Detecting such changes early in the process can help avoid unintended, negative consequences that could ultimately affect the security state of organizational information systems. The configuration change control element in this control enhancement reflects the change control elements defined by organizations in CM-3.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS IRM CAB Charter. **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP 800-124, 800-128; NIST IR 8062; FBI CJIS CSP v5.9	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; procedures addressing system configuration change control; configuration management plan; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with configuration change control responsibilities; organizational personnel with information security and privacy responsibilities; members of change control board or similar.

Test: Organizational processes for configuration change control.

CM-04: SECURITY IMPACT ANALYSIS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization analyzes changes to the system to determine potential security and privacy impacts prior to change implementation.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — All security-related information resources changes must be approved by the information owner through a change control process. [Source: DIR Control Standards Catalog CM-4]

Std.02 — Approval must occur prior to implementation by DFPS or independent contractors. [Source: DIR Control Standards Catalog CM-4]

Std.03 — Ensure that impact analyses address control system safety and security interdependencies. [Source: Catalog of Control Systems Security: Recommendations for Standards Developers]

Std.04 — If a proposed change has a significant effect on the security of the system, initiate re-authorization activities. Follow guidance in SP 800-37.

SUPPLEMENTAL GUIDANCE

Organizational personnel with information security responsibilities (e.g., Information System Administrators, Information System Security Officers, Information System Security Managers, and Information System Security Engineers) conduct security impact analyses. Individuals conducting security impact analyses possess the necessary skills/technical expertise to analyze the changes to information systems and the associated security ramifications. Security impact analysis may include, for example, reviewing security plans to understand security control requirements and reviewing system design documentation to understand control implementation and how specific changes might affect the controls. Security impact analyses may also include assessments of risk to better understand the impact of the changes and to determine if additional security controls are required. Security impact analyses are scaled in accordance with the security categories of the information system

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS IRM CAB Charter. **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP 800-128; FBI CJIS CSP v5.9	CA-7, CM-3, CM-8, CM-9, MA-2, RA-3, RA-5, RA-8, SA-5, SA-8, SA-10, SI-2.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; procedures addressing security impact analyses for changes to the system; procedures addressing privacy impact analyses for changes to the system; configuration management plan; security impact analysis documentation; privacy impact analysis documentation; privacy impact assessment; privacy risk assessment documentation, system design documentation; analysis tools and

associated outputs; change control records; system audit records; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with responsibility for conducting security impact analyses; organizational personnel with responsibility for conducting privacy impact analyses; organizational personnel with information security and privacy responsibilities; system developer; system/network administrators; members of change control board or similar.

Test: Organizational processes for security impact analyses; organizational processes for privacy impact analyses.

CM-04(01): SEPARATE TEST ENVIRONMENTS

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

For systems processing CJIS data, the following additional Implementation Standard applies:

The organization analyzes changes to the information system in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, compatibility, or intentional malice.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Test environments shall be kept either physically or logically separate from production environments. Copies of production data shall not be used for testing unless the data has been authorized for public release.

Std.02 — Confidential production data will not be used for testing purposes unless it has been de-classified/de-identified or a valid risk exception has been approved in accordance with IS-Controls section 2.4.3, Risk Acceptance. If an exception is approved to use confidential data for testing that cannot be de-classified/de-identified, the test environment must meet the same security control requirements as the production system and the confidential data must be removed from the non-production environment immediately upon completion of the required testing.

SUPPLEMENTAL GUIDANCE

Separate test environment in this context means an environment that is physically or logically isolated and distinct from the operational environment. The separation is sufficient to ensure that activities in the test environment do not impact activities in the operational environment, and information in the operational environment is not inadvertently transmitted to the test environment. Separate environments can be achieved by physical or logical means. If physically separate test environments are not used, organizations determine the strength of mechanism required when implementing logical separation (e.g., separation achieved through virtual machines).

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP 800-128; FBI CJIS CSP v5.9	SA-11, SC-7.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; procedures addressing security impact analyses for changes to the system; procedures addressing privacy impact analyses for changes to the system; configuration management plan; security impact analysis documentation; privacy impact analysis documentation; privacy impact assessment; privacy risk assessment documentation; analysis tools and associated outputs system design documentation; system architecture and configuration documentation; change control records; procedures addressing the authority to test with PII; system audit records; documentation of separate test and operational environments; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with responsibility for conducting security and privacy impact analyses; organizational personnel with information security and privacy responsibilities; system/network administrators; members of change control board or similar.

Test: Organizational processes for security and privacy impact analyses; automated mechanisms supporting and/or implementing security and privacy impact analyses of changes.

CM-04(02): VERIFICATION OF SECURITY FUNCTIONS

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

For systems processing CJIS data, the following additional Implementation Standard applies:

After system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Upon completion of a significant change, all relevant CJIS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable.

SUPPLEMENTAL GUIDANCE

Implementation in this context refers to installing changed code in the operational system that may have an impact on security or privacy controls.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP 800-128; FBI CJIS CSP v5.9	SA-11, SC-3, SI-6.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; procedures addressing security impact analyses for changes to the system; procedures addressing privacy impact analyses for changes to the system; privacy risk assessment documentation; configuration management plan; security and privacy impact analysis documentation; privacy impact assessment; analysis tools and associated outputs; change control records; control assessment results; system audit records; system component inventory; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with responsibility for conducting security and privacy impact analyses; organizational personnel with information security and privacy responsibilities; system/network administrators; security and privacy assessors.

Test: Organizational processes for security and privacy impact analyses; automated mechanisms supporting and/or implementing security and privacy impact analyses of changes.

CM-05: ACCESS RESTRICTIONS FOR CHANGE

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the system.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Limit personnel authorized to make changes to the infrastructure based on their job responsibilities and approve individuals prior to granting access.

SUPPLEMENTAL GUIDANCE

Any changes to the hardware, software, and/or firmware components of information systems can potentially have significant effects on the overall security of the systems. Therefore, organizations permit only qualified and authorized individuals to access information systems for purposes of initiating changes, including upgrades and modifications. Organizations maintain records of access to ensure that configuration change control is implemented and to support after-the-fact actions should organizations discover any unauthorized changes. Access restrictions for change also include software libraries. Access restrictions include, for example, physical and logical access controls (see AC-3 and PE-3), workflow automation, media libraries, abstract layers (e.g., changes implemented into third-party interfaces rather than directly into information systems), and change windows (e.g., changes occur only during specified times, making unauthorized changes easy to discover).

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** FIPS 140, 186; FBI CJIS CSP v5.9	AC-3, AC-5, AC-6, CM-9, PE-3, SC-28, SC-34, SC-37, SI-2, SI-10.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; procedures addressing access restrictions for changes to the system; configuration management plan; system design documentation; system architecture and configuration documentation; system configuration settings and associated documentation; logical access approvals; physical access approvals; access credentials; change control records; system audit records; system security plan; other relevant documents or records.

Interview: Organizational personnel with logical access control responsibilities; organizational personnel with physical access control responsibilities; organizational personnel with information security responsibilities; system/network administrators.

Test: Organizational processes for managing access restrictions to change; automated mechanisms supporting, implementing, or enforcing access restrictions associated with changes to the system.

CM-05(01): AUTOMATED ACCESS ENFORCEMENT / AUDITING

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

For systems processing CJIS data, the following additional Implementation Standard applies:

The information system enforces access restrictions and supports auditing of the enforcement actions.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — The information system:

a. Enforce access restrictions using automated mechanisms as identified in applicable System Security Plans (SSPs); and
b. Automatically generate audit records of the enforcement actions.

SUPPLEMENTAL GUIDANCE

Organizations log system accesses associated with applying configuration changes to ensure that configuration change control is implemented and to support after-the-fact actions should organizations discover any unauthorized changes.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** FIPS 140, 186; FBI CJIS CSP v5.9	AU-2, AU-6, AU-7, AU-12, CM-6, CM-11, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; procedures addressing access restrictions for changes to the system; system design documentation; system architecture and configuration documentation; system configuration settings and associated documentation; change control records; system audit records; system security plan; other relevant documents or records.

Interview: Organizational personnel with logical access control responsibilities; organizational personnel with physical access control responsibilities; organizational personnel with information security responsibilities; system/network administrators.

Test: Organizational processes for managing access restrictions to change; automated mechanisms implementing the enforcement of access restrictions for changes to the system; automated mechanisms supporting auditing of enforcement actions.

CM-05(02): REVIEW SYSTEM CHANGES

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

For systems processing CJIS data, the following additional Implementation Standard applies:

The information system enforces access restrictions and supports auditing of the enforcement actions.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — The information system:

a. Enforce access restrictions using automated mechanisms as identified in applicable System Security Plans (SSPs); and
b. Automatically generate audit records of the enforcement actions.

SUPPLEMENTAL GUIDANCE

Indications that warrant review of information system changes and the specific circumstances justifying such reviews may be obtained from activities carried out by organizations during the configuration change process.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** FIPS 140, 186; FBI CJIS CSP v5.9	AU-2, AU-6, AU-7, AU-12, CM-6, CM-11, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; procedures addressing access restrictions for changes to the system; system design documentation; system architecture and configuration documentation; system configuration settings and associated documentation; change control records; system audit records; system security plan; other relevant documents or records.

Interview: Organizational personnel with logical access control responsibilities; organizational personnel with physical access control responsibilities; organizational personnel with information security responsibilities; system/network administrators.

Test: Organizational processes for managing access restrictions to change; automated mechanisms implementing the enforcement of access restrictions for changes to the system; automated mechanisms supporting auditing of enforcement actions.

CM-05(05): LIMIT PRODUCTION / OPERATIONAL PRIVILEGES

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

For systems processing CJIS data, the following additional Implementation Standard applies:

The organization:

a. Limits privileges to change information system components and system-related information within a production or operational environment; and
b. Reviews and reevaluates privileges annually.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Enforce privileged access to change information system components and system-related information as defined in the applicable System Security Plans (SSPs) and reviews/reevaluates privileges annually.

SUPPLEMENTAL GUIDANCE

In many organizations, information systems support multiple core missions/business functions. Limiting privileges to change information system components with respect to operational systems is necessary because changes to a particular information system component may have far-reaching effects on mission/business processes supported by the system where the component resides. The complex, many-to-many relationships between systems and mission/business processes are in some cases, unknown to developers.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** FIPS 140, 186; FBI CJIS CSP v5.9	AC-2.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; procedures addressing access restrictions for changes to the system; configuration management plan; system design documentation; system architecture and configuration documentation; system configuration settings and associated documentation; user privilege reviews; user privilege recertifications; system component inventory; change control records; system audit records; system security plan; other relevant documents or records.

Interview: Organizational personnel with information security responsibilities; system/network administrators.

Test: Organizational processes for managing access restrictions to change; automated mechanisms supporting and/or implementing access restrictions for change.

CM-05(06): LIMIT LIBRARY PRIVILEGES

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

For systems processing CJIS data, the following additional Implementation Standard applies:

The organization limits privileges to change software resident within software libraries.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Enforce privileged access to change software resident within software libraries as defined in the applicable System Security Plans (SSPs).

SUPPLEMENTAL GUIDANCE

Software libraries include privileged programs.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** FIPS 140, 186; FBI CJIS CSP v5.9	AC-2.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; procedures addressing access restrictions for changes to the system; configuration management plan; system design documentation; system architecture and configuration documentation; system configuration settings and associated documentation; system component inventory; change control records; system audit records; system security plan; other relevant documents or records.

Interview: Organizational personnel with information security responsibilities; system/network administrators.

Test: Organizational processes for managing access restrictions to change; automated mechanisms supporting and/or implementing access restrictions for change

CM-06: CONFIGURATION SETTINGS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using approved common secure configurations derived from sources defined in Stds.02 & 03;
b. Implement the configuration settings;
c. Identify, document, and approve any deviations from established configuration settings for all configurable system components based on explicit operational requirements; and
d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS must:

a. Establish mandatory configuration settings for information technology products employed within the information system;
b. Configure the security settings of information technology products to the most restrictive mode consistent with operational requirements;
c. Document the configuration settings; and
d. Enforce the configuration settings in all components of the information system. [Source: DIR Control Standards Catalog CM-6]

Std.02 — All configuration baselines implemented in a production environment must be coordinated with and approved by DFPS Office of Information Security.

Std.03 — To resolve configuration conflicts among multiple security guidelines, follow the latest (current) guidance from the highest applicable source in the DFPS hierarchy as follows:

a. DFPS Information Security and Privacy Controls Catalog;
b. The Center for Internet Security (CIS);
c. NIST National Checklist Program (NCP) Repository;
d. Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG);
e. National Security Agency (NSA) STIGs; or

f. Vendor Configuration Baselines.

Std.04 — All configuration baselines used must be documented in the System Security Plan (SSP).

SUPPLEMENTAL GUIDANCE

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the information system that affect the security posture and/or functionality of the system. Information technology products for which security-related configuration settings can be defined include, for example, mainframe computers, servers (e.g., database, electronic mail, authentication, web, proxy, file, domain name), workstations, input/output devices (e.g., scanners, copiers, and printers), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications. Security-related parameters are those parameters impacting the security state of information systems including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: (i) registry settings; (ii) account, file, directory permission settings; and (iii) settings for functions, ports, protocols, services, and remote connections. Organizations establish organization-wide configuration settings and subsequently derive specific settings for information systems. The established settings become part of the systems configuration baseline.

Common secure configurations (also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, security technical implementation guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific information technology platforms/products and instructions for configuring those information system components to meet operational requirements. Common secure configurations can be developed by a variety of organizations including, for example, information technology product developers, manufacturers, vendors, consortia, academia, industry, federal agencies, and other organizations in the public and private sectors. Common secure configurations include the United States Government Configuration Baseline (USGCB) which affects the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and the defined standards within the protocol (e.g., Common Configuration Enumeration) provide an effective method to uniquely identify, track, and control configuration settings. OMB establishes federal policy on configuration requirements for federal information systems.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Configuration Management Policy. **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP 800-70, 800-126, 800-128; USGCB; NCPR; DOD STIG; FBI CJIS CSP v5.	AC-3, AC-19, AU-2, AU-6, CA-9, CM-2, CM-3, CM-5, CM-7, CM-11, CP-7, CP-9, CP-10, IA-3, IA-5, PL-8, PL-9, RA-5, SA-4, SA-5, SA-8, SA-9, SC-18, SC-28, SC-43, SI-2, SI-4, SI-6.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; procedures addressing configuration settings for the system; configuration management plan; system design documentation; system configuration settings and associated documentation; common secure configuration checklists; system component inventory; evidence supporting approved deviations from established configuration settings; change control records; system data processing and retention permissions; system audit records; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with security configuration management responsibilities; organizational personnel with privacy configuration management responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators/

Test: Organizational processes for managing configuration settings; automated mechanisms that implement, monitor, and/or control system configuration settings; automated mechanisms that identify and/or document deviations from established configuration settings.

CM-07: LEAST FUNCTIONALITY

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Configure the system to provide only mission-essential capabilities as identified in contingency plans and the System Security Plan (SSP); and
b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: all functions, ports, protocols, and/or services except those authorized and listed in the SSP.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Configure information systems to provide only essential capabilities. [Source: DIR Control Standards Catalog CM-7].

Std.02 — Actively monitor permitted ports, protocols, and services in accordance with the Continuous Monitoring Program (see CA-07).

Std.02 — Provide timely responses, as defined by the DFPS Chief Information Security Officer, to informational requests for organizational configuration status and posture information.

SUPPLEMENTAL GUIDANCE

Systems provide a wide variety of functions and services. Some of the functions and services routinely provided by default may not be necessary to support essential organizational missions, functions, or operations. Additionally, it is sometimes convenient to provide multiple services from a single system component but doing so increases risk over limiting the services provided by that single component. Where feasible, organizations limit component functionality to a single function per component. Organizations consider removing unused or unnecessary software and disabling unused or unnecessary physical and logical ports and protocols to prevent unauthorized connection of components, transfer of information, and tunneling. Organizations employ network scanning tools, intrusion detection and prevention systems, and end-point protection technologies, such as firewalls and host-based intrusion detection systems, to identify and prevent the use of prohibited functions, protocols, ports, and services. Least functionality can also be achieved as part of the fundamental design and development of the system (see SA-08, SC-02, and SC-03).

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Configuration Management Policy. **State:** DIR Security Control Standards Catalog. **Federal:** FIPS 140, 180, 186, 202; NIST SP 800-167; FBI CJIS CSP v5.9	AC-3, AC-19, AU-2, AU-6, CA-9, CM-2, CM-3, CM-5, CM-7, CM-11, CP-7, CP-9, CP-10, IA-3, IA-5, PL-8, PL-9, RA-5, SA-4, SA-5, SA-8, SA-9, SC-18, SC-28, SC-43, SI-2, SI-4, SI-6.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; procedures addressing least functionality in the system; configuration management plan; system design documentation; system configuration settings and associated documentation; system component inventory; common secure configuration checklists; system security plan; other relevant documents or records.

Interview: Organizational personnel with security configuration management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers.

Test: Organizational processes prohibiting or restricting functions, ports, protocols, software, and/or services; automated mechanisms implementing restrictions or prohibition of functions, ports, protocols, software, and/or services.

CM-07(01): PERIODIC REVIEW

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization:

a. Review the system quarterly or as system changes or incidents occur to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and
b. Disable or remove all functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Review the system quarterly or as defined in the System Security Plan to validate permitted ports, protocols, and services in accordance with the Continuous Monitoring Program (see CA-07).

SUPPLEMENTAL GUIDANCE

Organizations review functions, ports, protocols, and services provided by systems or system components to determine the functions and services that are candidates for elimination.

Such reviews are especially important during transition periods from older technologies to newer technologies (e.g., transition from IPv4 to IPv6). These technology transitions may require implementing the older and newer technologies simultaneously during the transition period and returning to minimum essential functions, ports, protocols, and services at the earliest opportunity. Organizations can either decide the relative security of the function, port, protocol, and/or service or base the security decision on the assessment of other entities. Unsecure protocols include Bluetooth, FTP, and peer-to-peer networking.

REFERENCES	**RELATED CONTROLS**

Agency: DFPS Information Security Policy; DFPS Configuration Management Policy. **State:** DIR Security Control Standards Catalog. **Federal:** FIPS 140, 180, 186, 202; NIST SP 800-167; FBI CJIS CSP v5.9	AC-18.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; procedures addressing least functionality in the system; configuration management plan; system design documentation; system configuration settings and associated documentation; common secure configuration checklists; documented reviews of functions, ports, protocols, and/or services; change control records; system audit records; system security plan; other relevant documents or records.

Interview: Organizational personnel with responsibilities for reviewing functions, ports, protocols, and services on the system; organizational personnel with information security responsibilities; system/network administrators; system developers.

Test: Organizational processes for reviewing or disabling functions, ports, protocols, and services on the system; automated mechanisms implementing review and disabling of functions, ports, protocols, and/or services.

CM-07(02): PREVENT PROGRAM EXECUTION

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The information system prevents program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions and rules authorizing the terms and conditions of software program usage.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Employ automated mechanisms to prevent program execution in accordance with defined lists of authorized programs (whitelists), defined lists of unauthorized programs (blacklists), access control policies, and CM-10.

SUPPLEMENTAL GUIDANCE

Prevention of program execution addresses organizational policies, rules of behavior, and/or access agreements that restrict software usage and the terms and conditions imposed by the developer or manufacturer, including software licensing and copyrights. Restrictions include prohibiting auto-execute features, restricting roles allowed to approve program execution, permitting, or prohibiting specific software programs, or restricting the number of program instances executed at the same time.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** FIPS 140, 180, 186, 202; NIST SP 800-167; FBI CJIS CSP v5.9	CM-8, PL-4, PL-9, PM-5, PS-6.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; procedures addressing least functionality in the system; configuration management plan; system design documentation; system configuration settings and associated documentation; system component inventory; common secure configuration checklists; specifications for preventing software program execution; change control records; system audit records; system security plan; other relevant documents or records.

Interview: Organizational personnel with information security responsibilities; system/network administrators; system developers.

Test: Organizational processes preventing program execution on the system; organizational processes for software program usage and restrictions; automated mechanisms preventing program execution on the system; automated mechanisms supporting and/or implementing software program usage and restrictions.

CM-07(03): REGISTRATION COMPLIANCE

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

For systems processing CJIS data, the following additional Implementation Standard applies:

The organization ensures compliance with CJIS-defined registration requirements for functions, ports, protocols, and services.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Review the system quarterly or as defined in the System Security Plan to validate CJIS-defined requirements for permitted ports, protocols, and services in accordance with the Continuous Monitoring Program (see CA-07).

SUPPLEMENTAL GUIDANCE

Organizations use the registration process to manage, track, and provide oversight for information systems and implemented functions, ports, protocols, and services

REFERENCES	RELATED CONTROLS

Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** FIPS 140, 180, 186, 202; NIST SP 800-167; FBI CJIS CSP v5.9	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System security plan; configuration management policy; procedures addressing least functionality in the system; configuration management plan; system configuration settings and associated documentation; system component inventory; audit and compliance reviews; system audit records; other relevant documents or record.

Interview: Organizational personnel with information security responsibilities; system/network administrators; system developers.

Test: Organizational processes ensuring compliance with registration requirements for functions, ports, protocols, and/or services; automated mechanisms implementing compliance with registration requirements for functions, ports, protocols, and/or services.

CM-07(04): UNAUTHORIZED SOFTWARE / DENYLIST

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

For systems processing CJIS data, the following additional Implementation Standard applies:

If software whitelisting is not implemented, the organization:

a. Identify software programs not authorized to execute on the system as identified in the System Security Plan (SSP);

b. Employ an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the system; and

c. Review and update the list of unauthorized software programs at least annually and when new threats are identified.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Configure systems to prevent installation or execution of unapproved, unauthorized, or unmanaged software; and to send alerts when such software is detected.

SUPPLEMENTAL GUIDANCE

Unauthorized software programs can be limited to specific versions or from a specific source. The concept of prohibiting the execution of unauthorized software may also be applied to user actions, system ports and protocols, IP addresses/ranges, websites, and MAC addresses.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** FIPS 140, 180, 186, 202; NIST SP 800-167; FBI CJIS CSP v5.9	CM-6, CM-8, CM-10, PL-9, PM-5.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; procedures addressing least functionality in the system; configuration management plan; system design documentation; system configuration settings and associated documentation; list of software programs not authorized to execute on the system; system component inventory; common secure configuration checklists; review and update records associated with list of unauthorized software programs; change control records; system audit records; system security plan; other relevant documents or records.

Interview: Organizational personnel with responsibilities for identifying software not authorized to execute on the system; organizational personnel with information security responsibilities; system/network administrators.

Test: Organizational process for identifying, reviewing, and updating programs not authorized to execute on the system; organizational process for implementing unauthorized software policy; automated mechanisms supporting and/or implementing unauthorized software policy.

CM-07(05): AUTHORIZED SOFTWARE / ALLOWLIST

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

For systems processing CJIS data, the following additional Implementation Standard applies:

The organization:

a. Identify software programs authorized to execute on the system as identified in the baseline configuration;
b. Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and
c. Review and update the list of authorized software programs annually.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Wherever applicable, employ application whitelisting technologies to permit the execution of explicitly allowed (whitelisted) software and block execution of everything else on systems and business networks; in particular, business servers such as mail servers and domain controllers.

SUPPLEMENTAL GUIDANCE

Authorized software programs can be limited to specific versions or from a specific source. To facilitate a comprehensive authorized software process and increase the strength of protection for attacks that bypass application level authorized software, software programs may be decomposed into and monitored at different levels of detail. These levels include applications, application programming interfaces, application modules, scripts, system processes, system services, kernel functions, registries, drivers, and dynamic link libraries. The concept of permitting the execution of authorized software may also be applied to user actions, system ports and protocols, IP addresses/ranges, websites, and MAC addresses. Organizations consider verifying the integrity of authorized software programs using digital signatures, cryptographic checksums, or hash functions. Verification of authorized software can occur either prior to execution or at system startup. The identification of authorized URLs for websites is addressed in SC-07.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** FIPS 140, 180, 186, 202; NIST SP 800-167; FBI CJIS CSP v5.9	CM-2, CM-6, CM-8, CM-10, PL-9, PM-5, SA-10, SC-34, SI-7.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; procedures addressing least functionality in the system; configuration management plan; system design documentation; system configuration settings and associated documentation; list of software programs authorized to execute on the system; system component inventory; common secure configuration checklists; review and update records associated with list of authorized software programs; change control records; system audit records; system security plan; other relevant documents or records.

Interview: Organizational personnel with responsibilities for identifying software authorized to execute on the system; organizational personnel with information security responsibilities; system/network administrator.

Test: Organizational process for identifying, reviewing, and updating programs authorized to execute on the system; organizational process for implementing authorized software policy; automated mechanisms supporting and/or implementing authorized software policy.

CM-08: INFORMATION SYSTEM COMPONENT INVENTORY

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a) Develop and document an inventory of system components that:
   1. Accurately reflects the system;
   2. Includes all components within the system;
   3. Does not include duplicate accounting of components or components assigned to any other system;
   4. Is at the level of granularity deemed necessary for tracking and reporting; and
   5. Includes the following information to achieve system component accountability: information as defined in Std.03 below; and

b. Review and update the system component inventory at least annually in accordance with PM-05, and whenever a change is made to the inventory.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS must develop, document, and maintain a current inventory of the components of the information system and relevant ownership information. [Source: DIR Control Standards Catalog CM-8]

Std.02 — Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. [Source: SP 800-171 3.4.1]

Std.03 — The inventory of information system components must include any information determined to be necessary by the organization to achieve effective property accountability including, but not limited to:

a. Manufacturer;
b. Type;
c. Model;
d. Serial Number;
e. Physical Location;
f. Software license information;
g. Information system/component owner;
h. Associated component configuration standard;
i. Software/firmware version information; and
j. Networked component/device machine name or network address.

Std.04 — The component inventory must be consistent with the authorization boundary of the system and is subject to annual review. All components within the authorization boundary of the system must be verified either as part of the system or recognized by another system as a component within that system.

SUPPLEMENTAL GUIDANCE

System components are discrete, identifiable information technology assets that include hardware, software, and firmware. Organizations may choose to implement centralized system component inventories that include components from all organizational systems. In such situations, organizations ensure that the inventories include system-specific information required for component accountability. The information necessary for effective accountability of system components includes the system name, software owners, software version numbers, hardware inventory specifications, software license information, and for networked components, the machine names and network addresses across all implemented protocols (e.g., IPv4, IPv6). Inventory specifications include date of receipt, cost, model, serial number, manufacturer, supplier information, component type, and physical location.

Preventing duplicate accounting of system components addresses the lack of accountability that occurs when component ownership and system association is not known, especially in large or complex connected systems. Effective prevention of duplicate accounting of system components necessitates use of a unique identifier for each component. For software inventory, centrally managed software that is accessed via other systems is addressed as a component of the system on which it is installed and managed. Software installed on multiple

organizational systems and managed at the system level is addressed for each individual system and may appear more than once in a centralized component inventory, necessitating a system association for each software instance in the centralized inventory to avoid duplicate accounting of components. Scanning systems implementing multiple network protocols (e.g., IPv4 and IPv6) can result in duplicate components being identified in different address spaces.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Configuration Management Policy. **State:** DIR Security Control Standards Catalog. **Federal:** OMB A-130; NIST SP 800-57-1, 800-57-2, 800-57-3, 800-128; NIST IR 8011-2, 8011-3; FBI CJIS CSP v5.9	CM-2, CM-7, CM-9, CM-10, CM-11, CM-13, CP-2, CP-9, MA-2, MA-6, PE-20, PL-9, PM-5, SA-4, SA-5, SI-2, SR-4.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; procedures addressing system component inventory; configuration management plan; system security plan; system design documentation; system component inventory; inventory reviews and update records; system security plan; other relevant documents or records.

Interview: Organizational personnel with component inventory management responsibilities; organizational personnel with information security responsibilities; system/network administrators.

Test: Organizational processes for managing the system component inventory; automated mechanisms supporting and/or implementing system component inventory.

CM-08(01): UPDATES DURING INSTALLATIONS / REMOVALS

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — When installing, updating, or removing an information system or infrastructure component, update system configuration needs to ensure an accurate inventory of supply chain protections. [Source: SP 800-161]

SUPPLEMENTAL GUIDANCE

Organizations can improve the accuracy, completeness, and consistency of system component inventories if the inventories are updated as part of component installations or removals or during general system updates. If

inventories are not updated at these key times, there is a greater likelihood that the information will not be appropriately captured and documented. System updates include hardware, software, and firmware components.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Configuration Management Policy. **State:** DIR Security Control Standards Catalog. **Federal:** OMB A-130; NIST SP 800-57-1, 800-57-2, 800-57-3, 800-128; NIST IR 8011-2, 8011-3; FBI CJIS CSP v5.9	PM-16.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; procedures addressing system component inventory; configuration management plan; system security plan; system component inventory; inventory reviews and update records; change control records; component installation records; component removal records; system security plan; other relevant documents or records.

Interview: Organizational personnel with component inventory updating responsibilities; organizational personnel with information security responsibilities; system/network administrators.

Test: Organizational processes for updating the system component inventory; automated mechanisms supporting and/or implementing system component inventory updates.

CM-08(02): AUTOMATED MAINTENANCE

Priority: P1

Baseline(s): High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.

AGENCY IMPLEMENTATION STANDARDS

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.01 - Maintain the currency, completeness, accuracy, and availability of the inventory of system components using automated mechanisms as identified in applicable System Security Plans (SSPs).

SUPPLEMENTAL GUIDANCE

Organizations maintain system inventories to the extent feasible. For example, virtual machines can be difficult to monitor because such machines are not visible to the network when not in use. In such cases, organizations maintain as up-to-date, complete, and accurate an inventory as is deemed reasonable. Automated maintenance

can be achieved by the implementation of CM-02(02) for organizations that combine system component inventory and baseline configuration activities.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Configuration Management Policy. **State:** DIR Security Control Standards Catalog. **Federal:** OMB A-130; NIST SP 800-57-1, 800-57-2, 800-57-3, 800-128; NIST IR 8011-2, 8011-3.	N/A.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; procedures addressing system component inventory; configuration management plan; system design documentation; system security plan; system component inventory; change control records; system maintenance records; system audit records; system security plan; other relevant documents or records.

Interview: Organizational personnel with component inventory management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers.

Test: Organizational processes for maintaining the system component inventory; automated mechanisms supporting and/or implementing the system component inventory.

CM-08(03): AUTOMATED UNAUTHORIZED COMPONENT DETECTION

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - Detect the presence of unauthorized hardware, software, and firmware components within the system using automated mechanisms as identified in the System Security Plan (SSP) continuously; and

Std.02 - Take the following actions when unauthorized components are detected: disable network access by such components; isolate the components; and notify personnel as identified in the incident response plan.

SUPPLEMENTAL GUIDANCE

Automated unauthorized component detection is applied in addition to the monitoring for unauthorized remote connections and mobile devices. Monitoring for unauthorized system components may be accomplished on an ongoing basis or by the periodic scanning of systems for that purpose. Automated mechanisms may also be used to prevent the connection of unauthorized components. Automated mechanisms can be implemented in systems

or in separate system components. When acquiring and implementing automated mechanisms, organizations consider whether such mechanisms depend on the ability of the system component to support an agent or supplicant in order to be detected since some types of components do not have or cannot support agents (e.g., IoT devices, sensors).

Isolation can be achieved, for example, by placing unauthorized system components in separate domains or subnets or quarantining such components. This type of component isolation is commonly referred to as "sandboxing."

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Configuration Management Policy. **State:** DIR Security Control Standards Catalog. **Federal:** OMB A-130; NIST SP 800-57-1, 800-57-2, 800-57-3, 800-128; NIST IR 8011-2, 8011-3; FBI CJIS CSP v5.9	AC-19, CA-7, RA-5, SC-3, SC-39, SC-44, SI-3, SI-4, SI-7.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; procedures addressing system component inventory; configuration management plan; system design documentation; system security plan; system component inventory; change control records; alerts/notifications of unauthorized components within the system; system monitoring records; system maintenance records; system audit records; system security plan; other relevant documents or records.

Interview: Organizational personnel with component inventory management responsibilities; organizational personnel with responsibilities for managing the automated mechanisms implementing unauthorized system component detection; organizational personnel with information security responsibilities; system/network administrators; system developers.

Test: Organizational processes for detection of unauthorized system components; organizational processes for taking action when unauthorized system components are detected; automated mechanisms supporting and/or implementing the detection of unauthorized system components; automated mechanisms supporting and/or implementing actions taken when unauthorized system components are detected.

CM-08(04): ACCOUNTABILITY INFORMATION

Priority: P1	
Baseline(s): High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization includes in the information system component inventory information, a means for identifying by position and role, and individuals responsible/accountable for administering those components.

AGENCY IMPLEMENTATION STANDARDS

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.01 - Include in the System Security Plan (SSP) component inventory information, a means for identifying by position or role at a minimum, individuals responsible and accountable for administering those components.

SUPPLEMENTAL GUIDANCE

Identifying individuals who are responsible and accountable for administering system components ensures that the assigned components are properly administered and that organizations can contact those individuals if some action is required (e.g., when the component is determined to be the source of a breach, needs to be recalled or replaced, or needs to be relocated).

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; **State:** DIR Security Control Standards Catalog. **Federal:** OMB A-130; NIST SP 800-57-1, 800-57-2, 800-57-3, 800-128; NIST IR 8011-2, 8011-3;	N/A.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; procedures addressing system component inventory; configuration management plan; system security plan; system component inventory; system security plan; other relevant documents or records.

Interview: Organizational personnel with component inventory management responsibilities; organizational personnel with information security responsibilities; system/network administrators.

Test: Organizational processes for managing the system component inventory; automated mechanisms supporting and/or implementing the system component inventory.

CM-09: CONFIGURATION MANAGEMENT PLAN

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization develops, documents, and implements a configuration management plan for the information system that:

a. Addresses roles, responsibilities, and configuration management processes and procedures;

b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;

c. Defines the configuration items for the system and places the configuration items under configuration management;

d. Is reviewed and approved by personnel as identified in the System Security Plan (SSP); and

e. Protects the configuration management plan from unauthorized disclosure and modification.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Establish and implement configuration standards that include a description of groups, roles, and responsibilities for management of network components.

Std.02 — Configuration management plans may be part of System Security Plans or maintained as separate documents. No system may be authorized for operation without a configuration management plan.

Std.03 — Responsibility for developing the configuration management process should not be assigned to personnel that are directly involved in information system development.

SUPPLEMENTAL GUIDANCE

Configuration management activities occur throughout the system development life cycle. As such, there are developmental configuration management activities (e.g., the control of code and software libraries) and operational configuration management activities (e.g., control of installed components and how the components are configured). Configuration management plans satisfy the requirements in configuration management policies while being tailored to individual systems. Configuration management plans define processes and procedures for how configuration management is used to support system development life cycle activities.

Configuration management plans are generated during the development and acquisition stage of the system development life cycle. The plans describe how to advance changes through change management processes; update configuration settings and baselines; maintain component inventories; control development, test, and operational environments; and develop, release, and update key documents.

Organizations can employ templates to help ensure the consistent and timely development and implementation of configuration management plans. Templates can represent a configuration management plan for the organization with subsets of the plan implemented on a system by system basis. Configuration management approval processes include the designation of key stakeholders responsible for reviewing and approving proposed changes to systems, and personnel who conduct security and privacy impact analyses prior to the implementation of changes to the systems. Configuration items are the system components, such as the hardware, software, firmware, and documentation to be configuration managed. As systems continue through the system development life cycle, new configuration items may be identified, and some existing configuration items may no longer need to be under configuration control.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP 800-128; FBI CJIS CSP v5.9	CM-2, CM-3, CM-4, CM-5, CM-8, PL-2, RA-8, SA-10, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; procedures addressing configuration management planning; configuration management plan; system design documentation; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with responsibilities for developing the configuration management plan; organizational personnel with responsibilities for implementing and managing processes defined in the configuration management plan; organizational personnel with responsibilities for protecting the configuration management plan; organizational personnel with information security and privacy responsibilities; system/network administrator.

Test: Organizational processes for developing and documenting the configuration management plan; organizational processes for identifying and managing configuration items; organizational processes for protecting the configuration management plan; automated mechanisms implementing the configuration management plan; automated mechanisms for managing configuration items; automated mechanisms for protecting the configuration management plan.

CM-10: SOFTWARE USAGE RESTRICTIONS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization:

a. Use software and associated documentation in accordance with contract agreements and copyright laws;
b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and
c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Acquire software only through known and reputable sources; maintain evidence of ownership of licenses and material; and carry out annual checks that only authorized software and licenses products are installed. [Source: Hitrust 06.b Intellectual Property Rights]

SUPPLEMENTAL GUIDANCE

Software license tracking can be accomplished by manual or automated methods, depending on organizational needs. Examples of contract agreements include software license agreements and non-disclosure agreements.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP 800-128; FBI CJIS CSP v5.9	AC-17, AU-6, CM-7, CM-8, PM-30, SC-7.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; software usage restrictions; software contract agreements and copyright laws; site license documentation; list of software usage restrictions; software license tracking reports; configuration management plan; system security plan; system security plan; other relevant documents or records.

Interview: Organizational personnel operating, using, and/or maintaining the system; organizational personnel with software license management responsibilities; organizational personnel with information security responsibilities; system/network administrators.

Test: Organizational processes for tracking the use of software protected by quantity licenses; organizational processes for controlling/documenting the use of peer-to-peer file sharing technology; automated mechanisms implementing software license tracking; automated mechanisms implementing and controlling the use of peer-to-peer files sharing technology.

CM-10(01): OPEN SOURCE SOFTWARE

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization establishes restrictions on the use of open source software. Open source software must:

a. Be legally licensed;
b. Be approved by DFPS Office of Information Security;
c. Adhere to a secure configuration baseline checklist from the U.S. Government or industry;
d. Be maintained and updated by information technology department on a consistent basis.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Acquire open-source software only through known and reputable sources and carry out regular checks that only authorized software and current products versions are installed.

SUPPLEMENTAL GUIDANCE

Open source software refers to software that is available in source code form. Certain software rights normally reserved for copyright holders are routinely provided under software license agreements that permit individuals to study, change, and improve the software. From a security perspective, the major advantage of open source software is that it provides organizations with the ability to examine the source code. However, there are also various licensing issues associated with open source software including, for example, the constraints on derivative use of such software.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Acceptable Use Agreement. **State:** DIR Security Control Standards Catalog. **Federal:** N/A	SI-7.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; software usage restrictions; software contract agreements and copyright laws; site license documentation; list of software usage restrictions; software license tracking reports; configuration management plan; system security plan; system security plan; other relevant documents or records.

Interview: Organizational personnel operating, using, and/or maintaining the system; organizational personnel with software license management responsibilities; organizational personnel with information security responsibilities; system/network administrators.

Test: Organizational processes for tracking the use of software protected by quantity licenses; organizational processes for controlling/documenting the use of peer-to-peer file sharing technology; automated mechanisms implementing software license tracking; automated mechanisms implementing and controlling the use of peer-to-peer files sharing technology.

CM-11: USER-INSTALLED SOFTWARE

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Establish configuration management and acceptable use policies governing the installation of software by users;
b. Enforce software installation policies through the following methods: organization-defined methods including system configuration settings and manual oversight; and
c. Monitor policy compliance at frequencies as specified in the Continuous Monitoring Program.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS must establish and enforce a policy governing the installation of software by users. [Source: DIR Control Standards Catalog CM-11]

Std.02 — Monitoring for user-installed software must be in compliance with information security continuous monitoring (ISCM) requirements.

SUPPLEMENTAL GUIDANCE

If provided the necessary privileges, users can install software in organizational systems. To maintain control over the software installed, organizations identify permitted and prohibited actions regarding software installation. Permitted software installations include updates and security patches to existing software and downloading new applications from organization- approved "app stores." Prohibited software installations include software with unknown or suspect pedigrees or software that organizations consider potentially malicious. Policies selected for governing user-installed software are organization-developed or provided by some external entity. Policy enforcement methods can include procedural methods and automated methods.

REFERENCES	RELATED CONTROLS

Agency: DFPS Information Security Policy; DFPS Acceptable Use Agreement. **State:** DIR Security Control Standards Catalog. **Federal:** FBI CJIS CSP v5.9	SI-7.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; procedures addressing user-installed software; configuration management plan; system security plan; system design documentation; system configuration settings and associated documentation; list of rules governing user installed software; system monitoring records; system audit records; continuous monitoring strategy; system security plan; other relevant documents or records.

Interview: Organizational personnel with responsibilities for governing user-installed software; organizational personnel operating, using, and/or maintaining the system; organizational personnel monitoring compliance with user-installed software policy; organizational personnel with information security responsibilities; system/network administrators.

Test: Organizational processes governing user-installed software on the system; automated mechanisms enforcing policies and methods for governing the installation of software by users; automated mechanisms monitoring policy compliance.

CM-12: INFORMATION LOCATION

Priority: P1

Baseline(s): Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization:

a. Identify and document the location of all DFPS information not classified as Public and the specific system components on which the information is processed and stored;

b. Identify and document the users who have access to the system and system components where the information is processed and stored; and

c. Document changes to the location (i.e., system or system components) where the information is processed and stored.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Identify and document the location of Confidental and Controlled data in the System Security Plan (SSP).

Std.02 — Identify and document users who have access to the system and system components and document changes in the System Security Plan (SSP).

SUPPLEMENTAL GUIDANCE	
Information location addresses the need to understand where information is being processed and stored. Information location includes identifying where specific information types and information reside in system components and how information is being processed so that information flow can be understood and adequate protection and policy management provided for such information and system components. The security category of the information is also a factor in determining the controls necessary to protect the information and the system component where the information resides (see FIPS 199). The location of the information and system components is also a factor in the architecture and design of the system (see SA-04, SA-08, SA-17).	
REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; **State:** DIR Security Control Standards Catalog. **Federal:** N/A	AC-2, AC-3, AC-4, AC-6, AC-23, CM-8, PM-5, RA-2, SA-4, SA-8, SA-17, SC-4, SC-16, SC-28, SI-4, SI-7.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; procedures addressing identification and documentation of information location; configuration management plan; system design documentation; system architecture documentation; PII inventory documentation; data mapping documentation; audit records; list of users with system and system component access; change control records; system component inventory; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with responsibilities for managing information location and user access to information; organizational personnel with responsibilities for operating, using, and/or maintaining the system; organizational personnel with information security and privacy responsibilities; system/network administrators; system developers.

Test: Organizational processes governing information location; automated mechanisms enforcing policies and methods for governing information location.

(CP) CONTINGENCY PLANNING

DFPS establishes, maintains, and effectively implements plans for emergency response, backup operations, and post-disaster recovery for DFPS information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

The CP control family includes controls specific to the DFPS contingency plan if a cybersecurity event should occur. This includes controls like contingency plan testing, updating, training, and backups, and system reconstitution.

The scope of these regulations and procedures in this Control are applicable to all information resources owned or operated by DFPS. The DFPS Business Continuity Planning Policy is applicable to all information resources owned or operated by DFPS.

The DFPS Chief Information Security Officer will review the Information System Contingency Plan & Disaster Recovery Plan at least annually and ensure the plan compliments other relevant Agency plans

and complies with Federal, State, and DFPS contingency and continuity of operations planning requirements.

CP-01: CONTINGENCY PLANNING POLICY AND PROCEDURES	
Priority: P1	
Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Develop, document, and disseminate to appropriate personnel:
   1. Organization-level contingency planning policy that:
      a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls;

b. Designate a senior management official as defined in the contingency planning policy to manage the development, documentation, and dissemination of the contingency planning policy and procedures; and

c. Review and update the current contingency planning:
   1. Policy every year and following major changes to legislation or security requirements; and
   2. Procedures every year and following major changes to legislation or security requirements.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Maintain written Continuity of Operations Plans that address information resources so that the effects of a disaster will be minimized, and the state organization will be able either to maintain or quickly resume mission-critical functions. [Source: DIR Control Standards Catalog CP-1]

Std.02 — The DFPS Chief Information Security Officer shall be responsible for:

a. Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks;

b. Providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities under 1 TAC 202; and

c. Developing and recommending policies and establishing procedures and practices, in cooperation with the agency Information Resources Manager, information-owners and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, or disclosure. [Source: 1 TAC 202.21(b)(3, 5, 8)]

SUPPLEMENTAL GUIDANCE

Contingency planning policy and procedures address the controls in the CP family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of contingency planning policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations.

Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to contingency planning policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP 800-12, 800-30, 800-34, 800-39, 800-50, 800-100; FBI CJIS CSP v5.9	PM-9, PS-8, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Contingency planning policy and procedures; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with contingency planning responsibilities; organizational personnel with information security and privacy responsibilities.

CP-02: CONTINGENCY PLAN

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization:

a. Develop a contingency plan for the system that:
   1. Identifies essential mission and business functions and associated contingency requirements;
   2. Provides recovery objectives, restoration priorities, and metrics;
   3. Addresses contingency roles, responsibilities, assigned individuals with contact information;
   4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure;
   5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented;
   6. Addresses the sharing of contingency information; and
   7. Is reviewed and approved by key personnel or roles and entities identified in the contingency plan;
b. Distribute copies of the contingency plan to key contingency personnel (identified by name and/or by role) and organizational elements as identified in the contingency plan;
c. Coordinate contingency planning activities with incident handling activities;
d. Review the contingency plan for the system at least annually as part of the annual risk assessment (see CP-04);
e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
f. Communicate contingency plan changes to key contingency personnel (identified by name and/or by role) and organizational elements as identified in the contingency plan;
g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and
h. Protect the contingency plan from unauthorized disclosure and modification.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — The plan shall be distributed to key personnel and a copy stored offsite. Elements of the plan for information resources shall include:

a. Business Impact Analysis to systematically assess the potential impacts of a loss of business functionality due to an interruption of computing and/or infrastructure support services resulting from various events or incidents. The analysis shall identify the following elements:
   1. Mission-Critical Information Resources (specific system resources required to perform critical functions) to include:
      a) Internal and external points of contact for personnel that provide or receive data or support interconnected systems.
      b) Supporting infrastructure such as electric power, telecommunications connections, and environmental controls.
   2. Disruption impacts and allowable outage times to include:
      a) Effects of an outage over time to assess the maximum allowable time that a resource may be denied before it prevents or inhibits the performance of an essential function.
      b) Effects of an outage across related resources and dependent systems to assess cascading effects on associated systems or processes.
   3. Recovery priorities that consider geographic areas, accessibility, security, environment, and cost and may include a combination of:
      a) Preventive controls and processes such as backup power, excess capacity, environmental sensors and alarms.
      b) Recovery techniques and technologies such as backup methodologies, alternate sites, software and hardware equipment replacement, implementation roles and responsibilities.

b. Risk Assessment to weigh the cost of implementing preventative measures against the risk of loss from not taking action.

c. Implementation, testing, and maintenance management program addressing the initial and ongoing testing and maintenance activities of the plan.

d. Disaster Recovery Plan — Each state organization shall maintain a written disaster recovery plan for major or catastrophic events that deny access to information resources for an extended period. Information learned from tests conducted since the plan was last updated will be used in updating the disaster recovery plan. The disaster recovery plan will:
   1. Contain measures which address the impact and magnitude of loss or harm that will result from an interruption;
   2. Identify recovery resources and a source for each;
   3. Contain step-by-step implementation instructions;
   4. Include provisions for annual testing. [Source: DIR Control Standards Catalog CP-2]

Std.02 — A single framework of business continuity plans shall be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance. [Source: Hitrust 12.d Business Continuity Planning Framework]

Std.03 — Define and document within contingency plans:

a. Maximum Tolerable Downtime (MTD) — The MTD represents the total amount of time organizations are willing to accept for a mission/business process outage or disruption and includes all impact considerations;

b. Recovery Time Objective (RTO) — RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business functions, and the MTD; and

c. Recovery Point Objective (RPO) — The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data shall be recovered (given the most recent backup copy of the data) after an outage.

Std.04 — Copies of the business continuity plans are distributed to the Information System Security Officer, System Owner, Contingency Plan Coordinator, System Administrator, and Database Administrator (or the organization's functional equivalents). [Source: Hitrust 12.c Developing and Implementing Continuity Plans Including Information Security]

SUPPLEMENTAL GUIDANCE

Contingency planning for systems is part of an overall program for achieving continuity of operations for organizational mission and business functions. Contingency planning addresses system restoration and implementation of alternative mission or business processes when systems are compromised or breached. Contingency planning is considered throughout the system development life cycle and is a fundamental part of the system design. Systems can be designed for redundancy, to provide backup capabilities, and for resilience. Contingency plans reflect the degree of restoration required for organizational systems since not all systems need to fully recover to achieve the level of continuity of operations desired. System recovery objectives reflect applicable laws, executive orders, directives, regulations, policies, standards, guidelines, organizational risk tolerance, and system impact level.

Actions addressed in contingency plans include orderly system degradation, system shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack. By coordinating contingency planning with incident handling activities, organizations ensure that the necessary planning activities are in place and activated in the event of an incident. Organizations consider whether continuity of operations during an incident conflicts with the capability to automatically disable the system. Incident response planning is part of contingency planning for organizations and is addressed in the IR (Incident Response) family.

REFERENCES	**RELATED CONTROLS**

Agency: DFPS Information Security Policy; **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP 800-34; NIST IR 8179.	CP-3, CP-4, CP-6, CP-7, CP-8, CP-9, CP-10, CP-11, CP-13, IR-4, IR-6, IR-8, IR-9, MA-6, MP-2, MP-4, MP-5, PL-2, PM-8, PM-11, SA-15, SA-20, SC-7, SC-23, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Contingency planning policy; procedures addressing contingency operations for the system; contingency plan; evidence of contingency plan reviews and updates; system security plan; other relevant documents or records.

Interview: Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel with incident handling responsibilities; organizational personnel with knowledge of requirements for mission and business functions; organizational personnel with information security responsibilities.

Test: Organizational processes for contingency plan development, review, update, and protection; automated mechanisms for developing, reviewing, updating, and/or protecting the contingency plan.

CP-02(01): COORDINATE WITH RELATED PLANS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization coordinates contingency plan development with organizational elements responsible for related plans.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Ensure that results of tests are shared with personnel responsible for related plans. Agency-wide full-scale simulations and exercises include personnel responsible for all applicable plans.

SUPPLEMENTAL GUIDANCE

Plans that are related to contingency plans include Business Continuity Plans, Disaster Recovery Plans, Critical Infrastructure Plans, Continuity of Operations Plans, Crisis Communications Plans, Insider Threat Implementation Plans, Data Breach Response Plans, Cyber Incident Response Plans, Breach Response Plans, and Occupant Emergency Plans.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; **State:** DIR Security Control Standards Catalog.	N/A

Federal: NIST SP 800-34; NIST IR 8179; FBI CJS CSP v5.9 Section 5.10.1.5	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Contingency planning policy; procedures addressing contingency operations for the system; contingency plan; business contingency plans; disaster recovery plans; continuity of operations plans; crisis communications plans; critical infrastructure plans; cyber incident response plan; insider threat implementation plans; occupant emergency plans; system security plan; other relevant documents or records.

Interview: Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel with information security responsibilities; personnel with responsibility for related plans.

CP-02(02): CAPACITY PLANNING

Priority: P1

Baseline(s): High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Ensure that capacity planning is incorporated into Contingency Plans.

a. Identify the services and resources facilitating obtaining necessary electronic covered information during an emergency, including staffing, non-information processing resources, as well as fallback arrangements for information processing facilities. Such fallback arrangements may include arrangements with third parties in the form of reciprocal agreements, or commercial subscription services. [Source: Hitrust CSF 12.c Developing and Implementing Continuity Plans Including Information Security]

SUPPLEMENTAL GUIDANCE

Capacity planning is needed because different types of threats (e.g., natural disasters, targeted cyber-attacks) can result in a reduction of the available processing, telecommunications, and support services originally intended to support the organizational missions/business functions. Organizations may need to anticipate degraded operations during contingency operations and factor such degradation into capacity planning.

REFERENCES	**RELATED CONTROLS**

Agency: DFPS Information Security Policy; **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP 800-34; NIST IR 8179.	PE-11, PE-12, PE-13, PE-14, PE-18, SC-5.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Contingency planning policy; procedures addressing contingency operations for the system; contingency plan; capacity planning documents; system security plan; other relevant documents or records.

Interview: Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel responsible for capacity planning; organizational personnel with information security responsibilities.

CP-02(03): RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS

Priority: P1

Baseline(s): Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization plans for the resumption of essential missions and business functions within the time period defined in the contingency plan of contingency plan activation.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Ensure that capacity planning is incorporated into Contingency Plans.

SUPPLEMENTAL GUIDANCE

Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. The time period for resumption of essential missions/business functions may be dependent on the severity/extent of disruptions to the information system and its supporting infrastructure.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP 800-34; NIST IR 8179; FBI CJS CSP v5.9 Section 5.10.1.5	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Contingency planning policy; procedures addressing contingency operations for the system; contingency plan; business impact assessment; system security plan; privacy plan; other related plans; system security plan; other relevant documents or records.

Interview: Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel with information security and privacy responsibilities; organizational personnel with knowledge of requirements for mission and business functions.

Test: Organizational processes for resumption of missions and business functions.

CP-02(05): CONTINUE ESSENTIAL MISSIONS / BUSINESS FUNCTIONS

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Ensure that the continuance of essential missions and business functions planning is incorporated into Contingency Plans.

SUPPLEMENTAL GUIDANCE

Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. The time period for resumption of essential missions/business functions may be dependent on the severity/extent of disruptions to the information system and its supporting infrastructure.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP 800-34; NIST IR 8179; FBI CJS CSP v5.9 Section 5.10.1.5	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Contingency planning policy; procedures addressing contingency operations for the system; contingency plan; business impact assessment; primary processing site agreements; primary storage site agreements; alternate processing site agreements; alternate storage site agreements; contingency plan test documentation; contingency plan test results; system security plan; other relevant documents or records.

Interview: Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel with knowledge of requirements for mission and business functions; organizational personnel with information security responsibilities.

Test: Organizational processes for continuing missions and business functions.

CP-02(08): IDENTIFY CRITICAL ASSETS

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization identifies critical information system assets supporting essential missions and business functions.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Criticality analysis is required for:

a. All moderate- and high-baseline systems in accordance with RA-09;
b. All systems supporting any essential mission or business function (see CP-02);
c. All systems identified in contingency plans.
d. Indicate whether assets are critical in System Security Plans (SSPs).

SUPPLEMENTAL GUIDANCE

Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. Organizations identify critical information system assets so that additional safeguards and countermeasures can be employed (above and beyond those safeguards and countermeasures routinely implemented) to help ensure that organizational missions/business functions can continue to be conducted during contingency operations. In addition, the identification of critical information assets facilitates the prioritization of organizational resources. Critical information system assets include technical and operational aspects. Technical aspects include, for example, information technology services, information system components, information technology products, and mechanisms. Operational aspects include, for example, procedures (manually executed operations) and personnel (individuals operating technical safeguards and/or executing manual procedures). Organizational program protection plans can provide assistance in identifying critical assets.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP 800-34; NIST IR 8179; FBI CJS CSP v5.9 Section 5.10.1.5	CM-8, RA-9.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Contingency planning policy; procedures addressing contingency operations for the system; contingency plan; business impact assessment; system security plan; other relevant documents or records.

Interview: Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel with knowledge of requirements for mission and business functions; organizational personnel with information security responsibilities.

CP-03: CONTINGENCY TRAINING

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Provide contingency training to system users consistent with assigned roles and responsibilities:
   1. Within 60 days of assuming a contingency role or responsibility;
   2. When required by system changes; and
   3. Review and update contingency training content annually and following major changes to legislation or security requirements.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Train personnel in their contingency roles and responsibilities with respect to the information system and provides periodic refresher training. [Source: DIR Control Standards Catalog CP-3]

SUPPLEMENTAL GUIDANCE

Contingency training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training. For example, some individuals may only need to know when and where to report for duty during contingency operations and if normal duties are affected; system administrators may require additional training on how to establish systems at alternate processing and storage sites; and organizational officials may receive more specific training on how to conduct mission-essential functions in designated off-site locations and how to establish communications with other governmental entities for purposes of coordination on contingency-related activities. Training for contingency roles or responsibilities reflects the specific continuity requirements in the contingency plan. Events that may precipitate an update to contingency training content include, but are not limited to, contingency plan testing or an actual contingency (lessons learned), assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. At the discretion of the organization, participation in a contingency plan test or exercise, including lessons learned sessions subsequent to the test or exercise, may satisfy contingency plan training requirements.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP 800-50; FBI CJS CSP v5.9 Section 5.2.1.4	AT-2, AT-3, AT-4, CP-2, CP-4, CP-8, IR-2, IR-4, IR-9.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Contingency planning policy; procedures addressing contingency training; contingency plan; contingency training curriculum; contingency training material; contingency training records; system security plan; other relevant documents or records.

Interview: Organizational personnel with contingency planning, plan implementation, and training responsibilities; organizational personnel with information security responsibilities.

Test: Organizational processes for contingency training.

CP-03(01): SIMULATED EVENTS

Priority: P1

Baseline(s): High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Train personnel in their contingency roles and responsibilities with respect to the information system and provide periodic refresher training. [Source: DIR Control Standards Catalog CP-3]

Std.02 — Document results of training and update contingency plans accordingly.

SUPPLEMENTAL GUIDANCE

The use of simulated events creates an environment for personnel to experience actual threat events, including cyber-attacks that disable websites, ransomware attacks that encrypt organizational data on servers, hurricanes that damage or destroy organizational facilities, or hardware or software failures.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP 800-50.	N/A.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Contingency planning policy; procedures addressing contingency training; contingency plan; contingency training curriculum; contingency training material; system security plan; other relevant documents or records.

Interview: Organizational personnel with contingency planning, plan implementation, and training responsibilities; organizational personnel with information security responsibilities.

Test: Organizational processes for contingency training; automated mechanisms for simulating contingency events.

CP-04: CONTINGENCY PLAN TESTING

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization:

a. Test the contingency plan for the system at the frequency specified in the contingency plan, at least annually using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: agency-approved tests as identified in the contingency plan.
b. Review the contingency plan test results; and
c. Initiate corrective actions, if needed.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — The written disaster recovery plan will include provisions for annual testing. [Source: DIR Control Standards Catalog CP-4]

Std.02 — Contingency plans for all new systems must be tested prior to the system's being deployed to an operational state in the production environment.

Std.03 — Major deficiencies discovered as a result of testing must be addressed in accordance with CA-05.

Std.04 —

a. A formal test need not be conducted if the organization actively exercises its contingency plan capability during real contingencies.
b. Any response capability not exercised during real contingencies must be formally tested.

SUPPLEMENTAL GUIDANCE

Business continuity plan tests ensure that all members of the recovery team and other relevant staff are aware of the plans and their responsibility for business continuity and information security and know their role when a plan is invoked.

The test schedule for business continuity plan(s) indicates how and when each element of the plan is tested. These techniques are applied on a 'programmatic' basis such that the tests build upon one another, and in a way that is relevant to the specific response and recovery plan. The results of tests are recorded and actions taken to

improve the plans, where necessary. Updates will also consider lessons learned from implementation of the business continuity plan(s). [Source: Hitrust 12.e Testing, Maintaining and Re-Assessing Business Continuity Plans]

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** FIPS 199; NIST SP 800-34, 800-84, 800-160-2.	AT-3, CP-2, CP-3, CP-8, CP-9, IR-3, IR-4, PL-2, PM-14, SR-2.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Contingency planning policy; procedures addressing contingency plan testing; contingency plan; contingency plan test documentation; contingency plan test results; system security plan; other relevant documents or records.

Interview: Organizational personnel with responsibilities for contingency plan testing, reviewing, or responding to contingency plan tests; organizational personnel with information security responsibilities.

Test: Organizational processes for contingency plan testing; automated mechanisms supporting the contingency plan and/or contingency plan testing.

CP-04(01): COORDINATE WITH RELATED PLANS

Priority: P1

Baseline(s): Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization coordinates contingency plan testing with organizational elements responsible for related plans.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Ensure that results of tests are shared with personnel responsible for related plans. Agency-wide full-scale simulations and exercises include personnel responsible for all applicable plans.

SUPPLEMENTAL GUIDANCE

Plans related to contingency planning for organizational systems include Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, and Occupant Emergency Plans. Coordination of contingency plan testing does not require organizations to create organizational elements to handle related plans or to align such elements with specific plans. However, it does require that if such organizational elements are responsible for related plans, organizations coordinate with those elements.

REFERENCES	RELATED CONTROLS

Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** FIPS 199; NIST SP 800-34, 800-84, 800-160-2.	IR-8, PM-8.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Contingency planning policy; incident response policy; procedures addressing contingency plan testing; contingency plan testing documentation; contingency plan; business continuity plans; disaster recovery plans; continuity of operations plans; crisis communications plans; critical infrastructure plans; cyber incident response plans; occupant emergency plans; system security plan; other relevant documents or records.

Interview: Organizational personnel with contingency plan testing responsibilities; personnel with responsibilities for related plans; organizational personnel with information security responsibilities.

CP-04(02): ALTERNATE PROCESSING SITE

Priority: P1

Baseline(s): High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization tests the contingency plan at the alternate processing site:

a. To familiarize contingency personnel with the facility and available resources; and
b. To evaluate the capabilities of the alternate processing site to support contingency operations.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Ensure that contingency plan tests are performed the alternate processing.

SUPPLEMENTAL GUIDANCE

Conditions at the alternate processing site may be significantly different than the conditions at the primary site. Having the opportunity to visit the alternate site and experience the actual capabilities available at the site can provide valuable information on potential vulnerabilities that could affect essential organizational mission and business functions. The on-site visit can also provide an opportunity to refine the contingency plan to address the vulnerabilities discovered during testing.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** FIPS 199; NIST SP 800-34, 800-84, 800-160-2.	CP-7.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Contingency planning policy; procedures addressing contingency plan testing; contingency plan; contingency plan test documentation; contingency plan test results; alternate processing site agreements; service-level agreements; system security plan; other relevant documents or records.

Interview: Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel with information security responsibilities.

Test: Organizational processes for contingency plan testing; automated mechanisms supporting the contingency plan and/or contingency plan testing.

CP-06: ALTERNATE STORAGE SITE

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and
b. Ensure that the alternate storage site provides controls equivalent to that of the primary site.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Mission-critical information must be backed up on a scheduled basis and stored off site in a secure, environmentally safe, locked facility accessible only to authorized DFPS representatives. [Source: DIR Control Standards Catalog CP-6]

Std.02 — Ensure that SLAs are consistent with contingency plans, including regional disaster event plans.

Std.03 — Document alternate storage sites in contingency plans.

Std.04 — If alternative temporary locations are used, the level of implemented security controls at these locations is to have logical and physical access controls that are equivalent to the primary site. [Source: Hitrust 12.c Developing and Implementing Continuity Plans Including Information Security]

SUPPLEMENTAL GUIDANCE

Alternate storage sites are geographically distinct from primary storage sites and maintain duplicate copies of information and data if the primary storage site is not available.

Similarly, alternate processing sites provide processing capability if the primary processing site is not available. Geographically distributed architectures that support contingency requirements may be considered alternate storage sites. Items covered by alternate storage site agreements include environmental conditions at the alternate sites, access rules for systems and facilities, physical and environmental protection requirements, and coordination of delivery and retrieval of backup media. Alternate storage sites reflect the requirements in

contingency plans so that organizations can maintain essential mission and business functions despite compromise, failure, or disruption in organizational systems.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP 800-34; FBI CJIS CSP v5.9	CP-2, CP-7, CP-8, CP-9, CP-10, MP-4, MP-5, PE-3, SC-36, SI-13.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Contingency planning policy; procedures addressing alternate storage sites; contingency plan; alternate storage site agreements; primary storage site agreements; system security plan; other relevant documents or records.

Interview: Organizational personnel with contingency plan alternate storage site responsibilities; organizational personnel with system recovery responsibilities; organizational personnel with information security responsibilities.

Test: Organizational processes for storing and retrieving system backup information at the alternate storage site; automated mechanisms supporting and/or implementing storage and retrieval of system backup information at the alternate storage site.

CP-06(01): SEPARATION FROM PRIMARY SITE

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — — Ensure that the risk of a disruption affecting both the primary and alternate storage site is low, or otherwise is at an acceptable level based on an assessment of risk, and document acceptance of risk in System Security Plans (SSPs).

SUPPLEMENTAL GUIDANCE

Threats that affect alternate storage sites are defined in organizational risk assessments and include natural disasters, structural failures, hostile attacks, and errors of omission or commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate storage sites based on the types of threats that are of concern. For threats such as hostile attacks, the degree of separation between sites is less relevant.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP 800-34; FBI CJIS CSP v5.9	RA-3.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Contingency planning policy; procedures addressing alternate storage sites; contingency plan; alternate storage site; alternate storage site agreements; primary storage site agreements; system security plan; other relevant documents or records.

Interview: Organizational personnel with contingency plan alternate storage site responsibilities; organizational personnel with system recovery responsibilities; organizational personnel with information security responsibilities.

CP-06(03): ACCESSIBILITY

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

AGENCY IMPLEMENTATION STANDARDS

Std.01 —Ensure that contingency planning identifies and documents potential accessibility difficulties to the alternate storage site in the event of an area-wide disruption or disaster.

SUPPLEMENTAL GUIDANCE

Area-wide disruptions refer to those types of disruptions that are broad in geographic scope with such determinations made by organizations based on organizational assessments of risk. Explicit mitigation actions include duplicating backup information at other alternate storage sites if access problems occur at originally designated alternate sites or planning for physical access to retrieve backup information if electronic accessibility to the alternate site is disrupted

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP 800-34; FBI CJIS CSP v5.9	RA-3.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Contingency planning policy; procedures addressing alternate storage sites; contingency plan; alternate storage site; alternate storage site agreements; primary storage site agreements; system security plan; other relevant documents or records.

Interview: Organizational personnel with contingency plan alternate storage site responsibilities; organizational personnel with system recovery responsibilities; organizational personnel with information security responsibilities.

CP-07: ALTERNATE PROCESSING SITE

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of all system operations identified in contingency plans for essential mission and business functions within a time period consistent with recovery time and recovery point objectives in accordance with CP-02 when the primary processing capabilities are unavailable;
b. Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption; and
c. Provide controls at the alternate processing site that are equivalent to those at the primary site.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Develop alternate processing site agreements (which may include Memoranda of Understanding (MOUs) and service level agreements (SLAs)) that are consistent with contingency plans.

Std.02 — Document alternate processing sites in contingency plans.

Std.03 — Alternate sites must be located sufficiently apart to prevent one disaster from affecting multiple facilities. The sites are designated either hot, warm, or cold based on the amount of time necessary to make the services available.

SUPPLEMENTAL GUIDANCE

Alternate processing sites are sites that are geographically distinct from primary processing sites. An alternate processing site provides processing capability in the event that the primary processing site is not available. Items covered by alternate processing site agreements include, for example, environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and coordination for the transfer/assignment of personnel. Requirements are specifically allocated to alternate processing sites that

reflect the requirements in contingency plans to maintain essential missions/business functions despite disruption, compromise, or failure in organizational information systems.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP 800-34; FBI CJIS CSP v5.9	CP-2, CP-6, CP-8, CP-9, CP-10, MA-6, PE-3, PE-11, PE-12, PE-17, SC-36, SI-13.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Contingency planning policy; procedures addressing alternate processing sites; contingency plan; alternate processing site agreements; primary processing site agreements; spare equipment and supplies inventory at alternate processing site; equipment and supply contracts; service-level agreements; system security plan; other relevant documents or records.

Interview: Organizational personnel with responsibilities for contingency planning and/or alternate site arrangements; organizational personnel with information security responsibilities,

Test: Organizational processes for recovery at the alternate site; automated mechanisms supporting and/or implementing recovery at the alternate processing site.

CP-08: TELECOMMUNICATIONS SERVICES

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization establishes alternate telecommunications services, including necessary agreements to permit the resumption of all system operations identified in contingency plans for essential mission and business functions within the time period specified in contingency plans when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Ensure alternate telecommunications Service Level Agreements (SLA) are in place to permit resumption of system Recovery Time Objectives (RTO) and business functions Maximum Tolerable Downtimes (MTD).

Std.02 — For systems that are rated as high baseline, ensure alternate telecommunications service agreements are in place to permit resumption of information system operations for essential missions and business functions within one (1) week of contingency plan activation when primary telecommunications capabilities are unavailable.

Std. 03 — Telecommunications restoration plans must provide adequate capabilities for channels of communication between the agency and other organizations involved in the coordination and support of the contingency plan. The contingency plan must document the following:

1. The timeframe for the alternate telecommunications services to begin providing telecommunications capabilities when the primary telecommunications capabilities are unavailable;
2. Channels for necessary communications within the agency and between the agency and other organizations involved;
3. The names of the primary and the alternate telecommunications services providers and points of contact; and
4. The agreements with the primary and alternate telecommunications service providers.

SUPPLEMENTAL GUIDANCE

Telecommunications services (for data and voice) for primary and alternate processing and storage sites are in scope for CP-08. Alternate telecommunications services reflect the continuity requirements in contingency plans to maintain essential mission and business functions despite the loss of primary telecommunications services. Organizations may specify different time periods for primary or alternate sites. Alternate telecommunications services include additional organizational or commercial ground-based circuits or lines, network-based approaches to telecommunications, or the use of satellites. Organizations consider factors such as availability, quality of service, and access when entering into alternate telecommunications agreements.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** 1 TAC 207.10; DIR Security Control Standards Catalog. **Federal:** NIST SP 800-34.	CP-2, CP-6, CP-7, CP-11, SC-7.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Contingency planning policy; procedures addressing alternate telecommunications services; contingency plan; primary and alternate telecommunications service agreements; system security plan; other relevant documents or records.

Interview: Organizational personnel with contingency plan telecommunications responsibilities; organizational personnel with system recovery responsibilities; organizational personnel with knowledge of requirements for mission and business functions; organizational personnel with information security responsibilities; organizational personnel with responsibility for acquisitions/contractual agreements.

Test: Automated mechanisms supporting telecommunications.

CP-08(01): PRIORITY OF SERVICE PROVISIONS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization:

a. Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and
b. Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Define priority-of-service provisions based on availability requirements and include in the telecommunications service agreement.

SUPPLEMENTAL GUIDANCE

Organizations consider the potential mission or business impact in situations where telecommunications service providers are servicing other organizations with similar priority of service provisions. Telecommunications Service Priority (TSP) is a Federal Communications Commission (FCC) program that directs telecommunications service providers (e.g., wireline and wireless phone companies) to give preferential treatment to users enrolled in the program when they need to add new lines or have their lines restored following a disruption of service, regardless of the cause. The FCC sets the rules and policies for the TSP program, and the Department of Homeland Security manages the TSP program. The TSP program is always in effect and not contingent on a major disaster or attack taking place. Federal sponsorship is required to enroll in the TSP program.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** 1 TAC 207.10; DIR Security Control Standards Catalog. **Federal:** NIST SP 800-34.	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Contingency planning policy; procedures addressing alternate telecommunications services; contingency plan; primary and alternate telecommunications service agreements; system security plan; other relevant documents or records.

Interview: Organizational personnel with contingency plan telecommunications responsibilities; organizational personnel with system recovery responsibilities; organizational personnel with knowledge of requirements for mission and business functions; organizational personnel with information security responsibilities; organizational personnel with responsibility for acquisitions/contractual agreements.

Test: Automated mechanisms supporting telecommunications.

CP-08(02): SINGLE POINTS OF FAILURE

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Ensure that the alternate telecommunication services (for example, telephone service) are separate from the primary service (for example, internet access) and does not share physical transmission equipment.

SUPPLEMENTAL GUIDANCE

In certain circumstances, telecommunications service providers or services may share the same physical lines, which increases the vulnerability of a single failure point. It is important to have provider transparency for the actual physical transmission capability for telecommunication services.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** 1 TAC 207.10; DIR Security Control Standards Catalog. **Federal:** NIST SP 800-34.	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Contingency planning policy; procedures addressing alternate telecommunications services; contingency plan; primary and alternate telecommunications service agreements; system security plan; other relevant documents or records.

Interview: Organizational personnel with contingency plan telecommunications responsibilities; organizational personnel with system recovery responsibilities; organizational personnel with knowledge of requirements for mission and business functions; organizational personnel with information security responsibilities; organizational personnel with responsibility for acquisitions/contractual agreements.

Test: Automated mechanisms supporting telecommunications.

CP-08(04): PROVIDER CONTINGENCY PLAN

Priority: P1

Baseline(s): High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization:

a. Requires primary and alternate telecommunications service providers to have contingency plans;

b. Reviews provider contingency plans to ensure that the plans meet organizational contingency requirements; and
c. Obtains evidence of contingency testing/training by providers within every 365 days.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — For systems marked as high baseline, reviews of provider contingency plans to ensure that the plans meet organizational contingency requirements and obtain evidence of contingency testing and training by providers annually.

SUPPLEMENTAL GUIDANCE

Reviews of provider contingency plans consider the proprietary nature of such plans. In some situations, a summary of provider contingency plans may be sufficient evidence for organizations to satisfy the review requirement. Telecommunications service providers may also participate in ongoing disaster recovery exercises in coordination with the Department of Homeland Security, state, and local governments. Organizations may use these types of activities to satisfy evidentiary requirements related to service provider contingency plan reviews, testing, and training.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** 1 TAC 207.10; DIR Security Control Standards Catalog. **Federal:** NIST SP 800-34.	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Contingency planning policy; procedures addressing alternate telecommunications services; contingency plan; primary and alternate telecommunications service agreements; system security plan; other relevant documents or records.

Interview: Organizational personnel with contingency plan telecommunications responsibilities; organizational personnel with system recovery responsibilities; organizational personnel with knowledge of requirements for mission and business functions; organizational personnel with information security responsibilities; organizational personnel with responsibility for acquisitions/contractual agreements.

Test: Automated mechanisms supporting telecommunications.

CP-09: INFORMATION SYSTEM BACKUP

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Conduct backups of user-level information contained in any component of the system at a frequency set in accordance with the system's recovery point objectives;
b. Conduct backups of system-level information contained in the system in accordance with the recovery point objective (RPO) as defined in the contingency plan (see CP-02);
c. Conduct backups of system documentation, including security- and privacy-related documentation when created or received, when updated, or as defined in the contingency plan, System Security Plan (SSP), or both when both are available; and
d. Protect the confidentiality, integrity, and availability of backup information.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Conduct backups of system-level information (including system state information) and critical user-level information contained in the information system and protect backup information at the storage location. [Source: DIR Control Standards Catalog CP-9]

Std.02 — Backups, including remote and cloud-based backups, must be compliant with DFPS requirements for encryption (see SC-13) and protecting data at rest (see SC-28).

SUPPLEMENTAL GUIDANCE

System-level information includes system state information, operating system software, middleware, application software, and licenses. User-level information includes information other than system-level information. Mechanisms employed to protect the integrity of system backups include digital signatures and cryptographic hashes. Protection of system backup information while in transit is addressed by MP-05 and SC-08. System backups reflect the requirements in contingency plans as well as other organizational requirements for backing up information. Organizations may be subject to laws, executive orders, directives, regulations, or policies with requirements regarding specific categories of information (e.g., personal health information). Organizational personnel consult with the senior agency official for privacy and legal counsel regarding such requirements.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** FIPS 140, 186; NIST SP 800-34, 800-130, 800-152; FBI CJIS CSP v5.9	CP-2, CP-6, CP-10, MP-4, MP-5, SC-8, SC-12, SC-13, SI-4, SI-13.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Contingency planning policy; procedures addressing system backup; contingency plan; backup storage location(s); system backup logs or records; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with system backup responsibilities; organizational personnel with information security and privacy responsibilities.

Test: Organizational processes for conducting system backups; automated mechanisms supporting and/or implementing system backup.

CP-10: INFORMATION SYSTEM RECOVERY AND RECONSTITUTION

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

Provide for the recovery and reconstitution of the system to a known state within the time period consistent with recovery time and recovery point objectives as defined in the contingency plan after a disruption, compromise, or failure.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Employ mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure. [Source: DIR Control Standards Catalog CP-10]
Std.02 — Recovery of the system after a failure or other contingency must be done in a trusted, secure, and verifiable manner.

Std.03 Secure information system recovery and reconstitution may include, but is not limited to:

1. Resetting all system parameters (either default or organization-established) to secure values;
2. Reinstalling patches;
3. Reestablishing configuration settings;
4. Reinstalling application and system software;
5. Loading information from the most recent, known secure backups; and
6. Testing the system.

SUPPLEMENTAL GUIDANCE

Recovery is executing contingency plan activities to restore organizational mission and business functions. Reconstitution takes place following recovery and includes activities for returning systems to fully operational states. Recovery and reconstitution operations reflect mission and business priorities; recovery point, recovery time, and reconstitution objectives; and organizational metrics consistent with contingency plan requirements. Reconstitution includes the deactivation of interim system capabilities that may have been needed during recovery operations. Reconstitution also includes assessments of fully restored system capabilities, reestablishment of continuous monitoring activities, system reauthorization (if required), and activities to prepare the system and organization for future disruptions, breaches, compromises, or failures. Recovery and reconstitution capabilities can include automated mechanisms and manual procedures. Organizations establish recovery time and recovery point objectives as part of contingency planning.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP 800-34; FBI CJIS CSP v5.9	CP-2, CP-4, CP-6, CP-7, CP-9, IR-4, SA-8, SC-24, SI-13.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Contingency planning policy; procedures addressing system backup; contingency plan; system backup test results; contingency plan test results; contingency plan test documentation; redundant secondary system for system backups; location(s) of redundant secondary backup system(s); system security plan; other relevant documents or records.

Interview: Organizational personnel with contingency planning, recovery, and/or reconstitution responsibilities; organizational personnel with information security responsibilities.

Test: Organizational processes implementing system recovery and reconstitution operations; automated mechanisms supporting and/or implementing system recovery and reconstitution operations.

CP-10(02): TRANSACTION RECOVERY

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The information system implements transaction recovery for systems that are transaction-based.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - Implement transaction recovery for information systems that are transaction-based.

SUPPLEMENTAL GUIDANCE

Transaction-based systems include database management systems and transaction processing systems. Mechanisms supporting transaction recovery include transaction rollback and transaction journaling.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP 800-34; FBI CJIS CSP v5.9	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Contingency planning policy; procedures addressing system recovery and reconstitution; contingency plan; system design documentation; system configuration settings and associated documentation; contingency plan test documentation; contingency plan test results; system transaction recovery records; system audit records; system security plan; other relevant documents or records.

Interview: Organizational personnel with responsibility for transaction recovery; organizational personnel with information security responsibilities.

Test: Automated mechanisms supporting and/or implementing transaction recovery capability.

(IA) IDENTIFICATION AND AUTHENTICATION

DFPS requires the identification of information system users, processes acting on behalf of users, or devices and authenticates (or verifies) the identities of those users, processes, or devices as a prerequisite to allowing access to DFPS information systems.

This Control applies to all DFPS information resources. The intended audience for this Control includes but is not limited to all information owners, managers, system administrators, and all users of DFPS information resources.

IA-01: IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Develop, document, and disseminate to appropriate personnel:
   1. Organization-level identification and authentication policy that:
      a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;
b. Designate a senior management official as defined in the identification and authentication policy to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; and
c. Review and update the current identification and authentication:
   1. Policy every year and following major changes to legislation or security requirements; and
   2. Procedures every year and following major changes to legislation or security requirements.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - Establish the policies for verifying the identity of a user, process, or device, as a prerequisite for granting access to resources in an information system. [Source: DIR Control Standards Catalog IA-1].

Std.02 — The DFPS Chief Information Security Officer is responsible for:

a. Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks;

b. Providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities under 1 TAC 202; and

c. Developing and recommending policies and establishing procedures and practices, in cooperation with the agency Information Resources Manager, information-owners and custodians, necessary to ensure the security

of information and information resources against unauthorized or accidental modification, destruction, or disclosure. [Source: 1 TAC 202.21(b)(3, 5, 8)]

SUPPLEMENTAL GUIDANCE

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the IA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** OMB A-130; FIPS 201; NIST SP 800-12, 800-30, 800-39, 800-63-3, 800-73-4, 800-76-2, 800-78-4, 800-100; NIST IR 7874; FBI CJIS CSP v5.9	AC-1, PM-9, PS-8, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy and procedures; system security plan; privacy plan; risk management strategy documentation; list of events requiring identification and authentication procedures to be reviewed and updated (e.g., audit findings); other relevant documents or records.

Interview: Organizational personnel with identification and authentication responsibilities; organizational personnel with information security and privacy responsibilities.

IA-02: IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

AGENCY IMPLEMENTATION STANDARDS

Std.01 - Each user of information resources shall be assigned a unique identifier except for situations where risk analysis demonstrates no need for individual accountability of users.

Std.02 — Each system's identification and authentication mechanisms must comply with the DFPS Identification and Authentication Standard.

SUPPLEMENTAL GUIDANCE

Organizations can satisfy the identification and authentication requirements by complying with the requirements in Homeland Security Presidential Directive 12. Organizational users include employees or individuals who organizations consider having an equivalent status to employees (e.g., contractors and guest researchers). Unique identification and authentication of users applies to all accesses other than those that are explicitly identified in AC-14 and that occur through the authorized use of group authenticators without individual authentication. Since processes execute on behalf of groups and roles, organizations may require unique identification of individuals in group accounts or for detailed accountability of individual activity.

Organizations employ passwords, physical authenticators, or biometrics to authenticate user identities or, in the case of multi-factor authentication, some combination thereof. Access to organizational systems is defined as either local access or network access. Local access is any access to organizational systems by users or processes acting on behalf of users, where access is obtained through direct connections without the use of networks. Network access is access to organizational systems by users (or processes acting on behalf of users) where access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. Internal networks include local area networks and wide area networks.

The use of encrypted virtual private networks for network connections between organization- controlled endpoints and non-organization-controlled endpoints may be treated as internal networks with respect to protecting the confidentiality and integrity of information traversing the network. Identification and authentication requirements for non-organizational users are described in IA-08.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Identification and Authentication Standard. **State:** DIR Security Control Standards Catalog. **Federal:** FIPS 140, 201, 202; NIST SP 800-63-3, 800-73-4, 800-76-2, 800-78-4, 800-79-2, 800-156, 800-166; NIST IR 7539, 7676, 7817, 7849, 7870, 7874, 7966; FBI CJIS CSP v5.9	AC-2, AC-3, AC-4, AC-14, AC-17, AC-18, AU-1, AU-6, IA-4, IA-5, IA-8, MA-4, MA-5, PE-2, PL-4, SA-4, SA-8.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; procedures addressing user identification and authentication; system security plan, system design documentation; system configuration settings and associated documentation; system audit records; list of system accounts; other relevant documents or records.

Interview: Organizational personnel with system operations responsibilities; organizational personnel with information security responsibilities; system/network administrators; organizational personnel with account management responsibilities; system developers.

Test: Organizational processes for uniquely identifying and authenticating users; automated mechanisms supporting and/or implementing identification and authentication capabilities.

IA-02(01): MULTI-FACTOR AUTHENTICATION TO PRIVILEGED ACCOUNTS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The information system implements multifactor authentication for network access to privileged accounts.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - For access to privileged accounts, implement multifactor authentication in accordance with the DFPS Identification and Authentication Standard.

SUPPLEMENTAL GUIDANCE

Multi-factor authentication requires the use of two or more different factors to achieve authentication. The authentication factors are defined as follows: something you know (e.g., a personal identification number (PIN)), something you have (e.g., a physical authenticator such as a cryptographic private key), or something you are (e.g., a biometric). Multi-factor authentication solutions that feature physical authenticators include hardware authenticators that provide time-based or challenge-response outputs and smart cards such as the U.S. Government Personal Identity Verification (PIV) card or the Department of Defense (DoD) Common Access Card (CAC). In addition to authenticating users at the system level (i.e., at logon), organizations may employ authentication mechanisms at the application level, at their discretion, to provide increased security. Regardless of the type of access (i.e., local, network, remote), privileged accounts are authenticated using multi-factor options appropriate for the level of risk. Organizations can add additional security measures, such as additional or more rigorous authentication mechanisms, for specific types of access.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Identification and Authentication Standard. **State:** DIR Security Control Standards Catalog. **Federal:** FIPS 140, 201, 202; NIST SP 800-63-3, 800-73-4, 800-76-2, 800-78-4, 800-79-2, 800-156, 800-166; NIST IR 7539, 7676, 7817, 7849, 7870, 7874, 7966; FBI CJIS CSP v5.9	AC-5, AC-6.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; procedures addressing user identification and authentication; system security plan; system design documentation; system configuration settings and associated documentation; system audit records; list of system accounts; other relevant documents or records.

Interview: Organizational personnel with system operations responsibilities; organizational personnel with account management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers.

Test: Automated mechanisms supporting and/or implementing multi-factor authentication capability.

IA-02(02): NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The information system implements multifactor authentication for network access to non-privileged accounts.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the DFPS network.

SUPPLEMENTAL GUIDANCE

Multi-factor authentication requires the use of two or more different factors to achieve authentication. The authentication factors are defined as follows: something you know (e.g., a personal identification number (PIN)), something you have (e.g., a physical authenticator such as a cryptographic private key), or something you are (e.g., a biometric). Multi-factor authentication solutions that feature physical authenticators include hardware authenticators that provide time-based or challenge-response outputs and smart cards such as the U.S. Government Personal Identity Verification card or the DoD Common Access Card. In addition to authenticating users at the system level, organizations may also employ authentication mechanisms at the application level, at their discretion, to provide increased information security. Regardless of the type of access (i.e., local, network, remote), non- privileged accounts are authenticated using multi-factor options appropriate for the level of risk. Organizations can provide additional security measures, such as additional or more rigorous authentication mechanisms, for specific types of access.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Identification and Authentication Standard. **State:** DIR Security Control Standards Catalog. **Federal:** FIPS 140, 201, 202; NIST SP 800-63-3, 800-73-4, 800-76-2, 800-78-4, 800-79-2, 800-156, 800-166; NIST IR 7539, 7676, 7817, 7849, 7870, 7874, 7966; FBI CJIS CSP v5.9	AC-5.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; system security plan; procedures addressing user identification and authentication; system design documentation; system configuration settings and associated documentation; system audit records; list of system accounts; other relevant documents or records

Interview: Organizational personnel with system operations responsibilities; organizational personnel with account management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers.

Test: Automated mechanisms supporting and/or implementing multi-factor authentication capability.

IA-02(03): LOCAL ACCESS TO PRIVILEGED ACCOUNTS

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

This control is withdrawn and Incorporated into IA-02(01) but still referenced in the FBI CJIS Security Policy v5.9. Please see IA-02(01).

IA-02(04): LOCAL ACCESS TO NON-PRIVILEGED ACCOUNTS

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

This control is withdrawn and Incorporated into IA-02(02) but still referenced in the FBI CJIS Security Policy v5.9. Please see IA-02(02).

IA-02(05): GROUP AUTHENTICATION

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Requiring individuals to use individual authenticators as a second level of authentication helps organizations to mitigate the risk of using group authenticators.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Identification and Authentication Standard. **State:** DIR Security Control Standards Catalog. **Federal:** FIPS 140, 201, 202; NIST SP 800-63-3, 800-73-4, 800-76-2, 800-78-4, 800-79-2, 800-156, 800-166; NIST IR 7539, 7676, 7817, 7849, 7870, 7874, 7966; FBI CJIS CSP v5.9	None.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; system security plan; procedures addressing user identification and authentication; system design documentation; system configuration settings and associated documentation; system audit records; list of system accounts; other relevant documents or records.

Interview: Organizational personnel with system operations responsibilities; organizational personnel with account management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers.

Test: Automated mechanisms supporting and/or implementing authentication capability for group accounts.

IA-02(06): NETWORK ACCESS TO PRIVILEGED ACCOUNTS - SEPARATE DEVICE

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The information system implements multifactor authentication for network access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets authentication assurance level (AAL) 2.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the DFPS network.

Std.02 - Where technically feasible, use authentication methods at authentication assurance level (AAL) 2 or 3.. [Source: NIST SP 800-63B]

SUPPLEMENTAL GUIDANCE

The purpose of requiring a device that is separate from the system to which the user is attempting to gain access for one of the factors during multi-factor authentication is to reduce the likelihood of compromising authenticators or credentials stored on the system. Adversaries may be able to compromise such authenticators

or credentials and subsequently impersonate authorized users. Implementing one of the factors on a separate device (e.g., a hardware token), provides a greater strength of mechanism and an increased level of assurance in the authentication process.

SP 800-63B Section 4.5 summarizes the combinations of authenticators that can meet the requirements of AAL2.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Identification and Authentication Standard. **State:** DIR Security Control Standards Catalog. **Federal:** FIPS 140, 201, 202; NIST SP 800-63-3, 800-63B, 800-73-4, 800-76-2, 800-78-4, 800-79-2, 800-156, 800-166; NIST IR 7539, 7676, 7817, 7849, 7870, 7874, 7966; FBI CJIS CSP v5.9	AC-6.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; system security plan; procedures addressing user identification and authentication; system design documentation; system configuration settings and associated documentation; system audit records; list of system accounts; other relevant documents or records.

Interview: Organizational personnel with system operations responsibilities; organizational personnel with account management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers.

Test: Automated mechanisms supporting and/or implementing multi-factor authentication capability.

IA-02(08): NETWORK ACCESS TO PRIVILEGED ACCOUNTS - REPLAY RESISTANT

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - Where technically feasible, use authentication methods at authentication assurance level (AAL) 2 and 3. AAL2 and AAL3 use either nonce or challenges and are resistant to replay attacks.

SUPPLEMENTAL GUIDANCE

A "replay-resistant" authentication mechanism is one that prevents someone who is snooping on network traffic from being able to store and re-use at a later time. Examples of replay-resistant authenticators are OTP devices, cryptographic authenticators, and look-up secrets. In contrast, memorized secrets are not considered replay resistant because the authenticator output — the secret itself — is provided for each authentication.

Authentication processes resist replay attacks if it is impractical to achieve successful authentications by replaying previous authentication messages. Replay-resistant techniques include, for example, protocols that use nonces or challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Identification and Authentication Standard. **State:** DIR Security Control Standards Catalog. **Federal:** FIPS 140, 201, 202; NIST SP 800-63-3, 800-73-4, 800-76-2, 800-78-4, 800-79-2, 800-156, 800-166; NIST IR 7539, 7676, 7817, 7849, 7870, 7874, 7966; FBI CJIS CSP v5.9	None.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; system security plan; procedures addressing user identification and authentication; system design documentation; system configuration settings and associated documentation; system audit records; list of privileged system accounts; other relevant documents or records.

Interview: Organizational personnel with system operations responsibilities; organizational personnel with account management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers.

Test: Automated mechanisms supporting and/or implementing identification and authentication capabilities; automated mechanisms supporting and/or implementing replay-resistant authentication mechanisms.

IA-02(09): NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS - REPLAY RESISTANT

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

This control is withdrawn and incorporated into IA-02(08) but still referenced in the FBI CJIS Security Policy v5.9. Please see IA-02(08).

IA-02(11): REMOTE ACCESS - SEPARATE DEVICE

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

This control is withdrawn and incorporated into IA-02(06) but still referenced in the FBI CJIS Security Policy v5.9. Please see IA-02(06).

IA-02(12): ACCEPTANCE OF PIV CREDENTIALS

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The information system accepts and electronically verifies PIV credentials.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - DFPS use access cards to control access to information systems at the appropriate security level.

SUPPLEMENTAL GUIDANCE

Acceptance of Personal Identity Verification (PIV)-compliant credentials applies to organizations implementing logical access control and physical access control systems. PIV-compliant credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. The adequacy and reliability of PIV card issuers are authorized using [SP 800-79-2]. Acceptance of PIV-compliant credentials includes derived PIV credentials, the use of which is addressed in [SP 800-166]. The DOD Common Access Card (CAC) is an example of a PIV credential.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Identification and Authentication Standard. **State:** DIR Security Control Standards Catalog. **Federal:** FIPS 140, 201, 202; NIST SP 800-63-3, 800-73-4, 800-76-2, 800-78-4, 800-79-2, 800-156, 800-166; NIST IR 7539, 7676, 7817, 7849, 7870, 7874, 7966; FBI CJIS CSP v5.9	None.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; system security plan; procedures addressing user identification and authentication; system design documentation; system configuration settings and associated documentation; system audit records; PIV verification records; evidence of PIV credentials; PIV credential authorizations; other relevant documents or records.

Interview: Organizational personnel with system operations responsibilities; organizational personnel with account management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers.

Test: Automated mechanisms supporting and/or implementing acceptance and verification of PIV credentials.

IA-02(13): OUT-OF-BAND AUTHENTICATION

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The information system implements out-of-band authentication identified in standard 1 under out-of-band authentication is used as an advanced authentication method.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - Authenticator is sent on demand via text message, authenticator application, etc. (CJIS 5.6.2.2)

Std.02 - Where technically feasible, use authentication methods at authentication assurance level (AAL) 2 or 3.. [Source: NIST SP 800-63B]

SUPPLEMENTAL GUIDANCE

Out-of-band authentication (OOBA) refers to the use of two separate communication paths to identify and authenticate users or devices to an information system. The first path (i.e., the in-band path), is used to identify and authenticate users or devices, and generally is the path through which information flows. The second path (i.e., the out-of-band path) is used to independently verify the authentication and/or requested action. For example, a user authenticates via a notebook computer to a remote server to which the user desires access and requests some action of the server via that communication path. Subsequently, the server contacts the user via the user's cell phone to verify that the requested action originated from the user. The user may either confirm the intended action to an individual on the telephone or provide an authentication code via the telephone. This type of authentication can be employed by organizations to mitigate actual or suspected man-in the-middle attacks. The conditions for activation can include, for example, suspicious activities, new threat indicators or elevated threat levels, or the impact level or classification level of information in requested transactions.

REFERENCES	RELATED CONTROLS

Agency: DFPS Information Security Policy; DFPS Identification and Authentication Standard. **State:** DIR Security Control Standards Catalog. **Federal:** FIPS 140, 201, 202; NIST SP 800-63-3, 800-73-4, 800-76-2, 800-78-4, 800-79-2, 800-156, 800-166; NIST IR 7539, 7676, 7817, 7849, 7870, 7874, 7966; FBI CJIS CSP v5.9	IA-10, IA-11, SC-37.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; system security plan; procedures addressing user identification and authentication; system design documentation; system configuration settings and associated documentation; system audit records; system-generated list of out-of-band authentication paths; other relevant documents or records.

Interview: Organizational personnel with system operations responsibilities; organizational personnel with account management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers.

Test: Automated mechanisms supporting and/or implementing out-of-band authentication capability.

IA-03: DEVICE IDENTIFICATION AND AUTHENTICATION

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The information system uniquely identifies and authenticates all network-connected endpoint devices before establishing a remote or network connection.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - Document the protocols used for device identification and authentication in the applicable System Security Plan (SSP).

SUPPLEMENTAL GUIDANCE

Organizational devices requiring unique device-to-device identification and authentication may be defined by type, by device, or by a combination of type/device. Information systems typically use either shared known information (e.g., Media Access Control [MAC] or Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for device identification or organizational authentication solutions (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP], Radius server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify/authenticate devices on local and/or wide area networks. Organizations determine the required strength of authentication mechanisms by the security categories of information systems. Because of the challenges of applying this control on large scale, organizations are encouraged to only apply the control to those limited number (and type) of devices that truly need to support this capability.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** FBI CJIS CSP v5.9	AC-17, AC-18, AC-19, AU-6, CA-3, CA-9, IA-4, IA-5, IA-9, IA-11, SI-4.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; system security plan; procedures addressing device identification and authentication; system design documentation; list of devices requiring unique identification and authentication; device connection reports; system configuration settings and associated documentation; other relevant documents or records.

Interview: Organizational personnel with operational responsibilities for device identification and authentication; organizational personnel with information security responsibilities; system/network administrators; system developers.

Test: Automated mechanisms supporting and/or implementing device identification and authentication capabilities.

IA-03(01): CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The information system authenticates devices and/or types of devices before establishing remote or network connection using bidirectional authentication that is cryptographically based.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - Document the protocols used for device identification and authentication in the applicable System Security Plan (SSP).

SUPPLEMENTAL GUIDANCE

Bidirectional authentication provides a means for both connecting parties to mutually authenticate one another, and cryptographic authentication provides a secure means of authenticating without the use of clear text passwords. For example, a client and a server using mutual authentication take steps to independently verify each other's identity, instead of only the client authenticating the server.

A local connection is any connection with a device communicating without the use of a network. A network connection is any connection with a device that communicates through a network (e.g., local area or wide area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Bidirectional authentication provides stronger safeguards to validate the identity of other devices for connections that are of greater risk (e.g., remote connections).

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** FBI CJIS CSP v5.9	SC-8, SC-12, SC-13.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; system security plan; procedures addressing device identification and authentication; system design documentation; list of devices requiring unique identification and authentication; device connection reports; system configuration settings and associated documentation; other relevant documents or record.

Interview: Organizational personnel with operational responsibilities for device identification and authentication; organizational personnel with information security responsibilities; system/network administrators; system developers.

Test: Automated mechanisms supporting and/or implementing device authentication capability; cryptographically based bidirectional authentication mechanisms.

IA-03(04): DEVICE ATTESTATION

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

For systems processing CJIS data, the following additional Implementation Standard applies:

Handle device identification and authentication based on attestation by configuration management process.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - Document the protocols used for device identification and authentication in the applicable System Security Plan (SSP).

Std.02 – Where technically feasible, use Azure AD to identify and authenticate Azure AD Registered, Azure AD Joined, and Azure AD Hybrid joined devices.

SUPPLEMENTAL GUIDANCE

Device attestation refers to the identification and authentication of a device based on its configuration and known operating state. This might be determined via some cryptographic hash of the device. If device attestation is the means of identification and authentication, then it is important that patches and updates to the device are handled via a configuration management process such that the those patches/updates are done securely and at the same time do not disrupt the identification and authentication to other devices.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** FBI CJIS CSP v5.9	CM-2, CM-3, CM-6.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; system security plan; procedures addressing device identification and authentication; procedures addressing device configuration management; system design documentation; system configuration settings and associated documentation; configuration management records; change control records; system audit records; other relevant documents or records.

Interview: Organizational personnel with operational responsibilities for device identification and authentication; organizational personnel with information security responsibilities; system/network administrators.

Test: Automated mechanisms supporting and/or implementing device identification and authentication capabilities; automated mechanisms supporting and/or implementing configuration management; cryptographic mechanisms supporting device attestation.

IA-04: IDENTIFIER MANAGEMENT

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization manages information system identifiers by:

a. Receiving authorization from personnel or roles as defined in the applicable System Security Plan (SSP) to assign an individual, group, role, service, or device identifier;
b. Selecting an identifier that identifies an individual, group, role, service, or device;
c. Assigning the identifier to the intended individual, group, role, service, or device; and
d. Preventing reuse of identifiers for at least one year for individuals, groups, roles, services, or devices.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - A user's access authorization shall be appropriately modified or removed when the user's employment or job responsibilities within the state organization change. [Source: DIR Control Standards Catalog IA-4]

Std.02 – Sensitive Personal Information, to include SSNs and parts of SSNs, must not be used as system identifiers. Identifier management must ensure that any access to, or action involving, personally identifiable information (PII) is attributable to a unique individual.

SUPPLEMENTAL GUIDANCE

Common device identifiers include Media Access Control (MAC) addresses, Internet Protocol (IP) addresses, or device-unique token identifiers. The management of individual identifiers is not applicable to shared system

accounts. Typically, individual identifiers are the usernames of the system accounts assigned to those individuals. In such instances, the account management activities of AC-02 use account names provided by IA-04. Identifier management also addresses individual identifiers not necessarily associated with system accounts. Preventing the reuse of identifiers implies preventing the assignment of previously used individual, group, role, service, or device identifiers to different individuals, groups, roles, services, or devices.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Account Management Policy. **State:** DIR Security Control Standards Catalog. **Federal:** FIPS 201; NIST SP 800-63-3, 800-73-4, 800-76-2, 800-78-4; FBI CJIS CSP v5.9	AC-5, IA-2, IA-3, IA-5, IA-8, IA-9, IA-12, MA-4, PE-2, PE-3, PE-4, PL-4, PM-12, PS-3, PS-4, PS-5, SC-37.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; procedures addressing identifier management; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of system accounts; list of identifiers generated from physical access control devices; other relevant documents or records.

Interview: Organizational personnel with identifier management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers.

Test: Automated mechanisms supporting and/or implementing identifier management.

IA-04(02): SUPERVISOR AUTHORIZATION

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

This control is withdrawn and incorporated into IA-12(01) but still referenced in the FBI CJIS Security Policy v5.9. Please see IA-12(01).

IA-04(04): IDENTIFY USER STATUS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

For systems processing CJIS data, the following additional Implementation Standard applies:

Manage individual identifiers by uniquely identifying each individual as possessing (or not possessing) specific individual status characteristics including, but not limited to, contractor or foreign national.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Characteristics that identify the status of individuals include contractors, foreign nationals, and non-organizational users. Identifying the status of individuals by these characteristics provides additional information about the people with whom organizational personnel are communicating. For example, it might be useful for a government employee to know that one of the individuals on an email message is a contractor.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** FIPS 201; NIST SP 800-63-3, 800-73-4, 800-76-2, 800-78-4; FBI CJIS CSP v5.9	AC-5, IA-2, IA-3, IA-5, IA-8, IA-9, IA-12, MA-4, PE-2, PE-3, PE-4, PL-4, PM-12, PS-3, PS-4, PS-5, SC-37.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; system security plan; procedures addressing identifier management; procedures addressing account management; list of characteristics identifying individual status; other relevant documents or records.

Interview: Organizational personnel with identifier management responsibilities; organizational personnel with information security responsibilities; system/network administrators.

Test: Automated mechanisms supporting and/or implementing identifier management.

IA-05: AUTHENTICATOR MANAGEMENT

Priority: P1	
Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization manages information system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;
b. Establishing initial authenticator content for any authenticators issued by the organization;
c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;
e. Changing default authenticators prior to first use;
f. Changing or refreshing authenticators at the frequency defined in the DFPS Identification and Authentication Standard or when major changes to legislation or security requirements occur;
g. Protecting authenticator content from unauthorized disclosure and modification;
h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and
i. Changing authenticators for group or role accounts when membership to those accounts' changes.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Organization must manage information system authenticators by:

a. Defining initial authenticator content;

b. Establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; and

c. Changing default authenticators upon information system installation. [Source: DIR Control Standards Catalog IA-5]

Std.02 — Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.

SUPPLEMENTAL GUIDANCE

Authenticators include passwords, cryptographic devices, biometrics, certificates, one-time password devices, and ID badges. Device authenticators include certificates and passwords. Initial authenticator content is the actual content of the authenticator (e.g., the initial password). In contrast, the requirements for authenticator content contain specific criteria or characteristics (e.g., minimum password length). Developers may deliver system components with factory default authentication credentials (i.e., passwords) to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant risk. The requirement to protect individual authenticators may be implemented via control PL-04 or PS-06 for authenticators in the possession of individuals and by controls AC-03, AC-06, and SC-28 for authenticators stored in organizational systems, including passwords stored in hashed or encrypted formats or files containing encrypted or hashed passwords accessible with administrator privileges.

Systems support authenticator management by organization-defined settings and restrictions for various authenticator characteristics (e.g., minimum password length, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication). Actions can be taken to safeguard individual authenticators, including maintaining possession of authenticators, not sharing authenticators with others, and immediately reporting lost, stolen, or compromised authenticators. Authenticator management includes issuing and revoking authenticators for temporary access when no longer needed.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Account Management Policy. **State:** DIR Security Control Standards Catalog.	AC-3, AC-6, CM-6, IA-2, IA-4, IA-7, IA-8, IA-9, MA-4, PE-2, PL-4, SC-12, SC-13.

Federal: FIPS 140, 180, 201, 202; NIST SP 800-63-3, 800-73-4, 800-76-2, 800-78-4; NIST IR 7539, 7817, 7849, 7870, 8040; FBI CJIS CSP v5.9	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; system security plan; addressing authenticator management; system design documentation; system configuration settings and associated documentation; list of system authenticator types; change control records associated with managing system authenticators; system audit records; other relevant documents or records.

Interview: Organizational personnel with authenticator management responsibilities; organizational personnel with information security responsibilities; system/network administrators.

Test: Automated mechanisms supporting and/or implementing authenticator management capability.

IA-05(01): PASSWORD-BASED AUTHENTICATION

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

For password-based authentication:

a. Maintain a list of commonly used, expected, or compromised passwords and update the list at least every 90 days and when organizational passwords are suspected to have been compromised directly or indirectly;
b. Verify, when users create or update passwords, that the passwords are not found on the list of commonly used, expected, or compromised passwords in IA-05(01)a;
c. Transmit passwords only over cryptographically protected channels;
d. Store passwords using an approved salted key derivation function, preferably using a keyed hash;
e. Require immediate selection of a new password upon account recovery;
f. Allow user selection of long passwords and passphrases, including spaces and all printable characters;
g. Employ automated tools to assist the user in selecting strong password authenticators; and
h. Enforce the following composition and complexity rules: composition and complexity rules in accordance with the DFPS Identification and Authentication Standard.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — This control applies only to systems that use a memorized secret (passphrase, PIN, etc.).

Std.02 — For all requirements concerning the use of memorized secrets, see the DFPS Identification and Authentication Standard.

SUPPLEMENTAL GUIDANCE

Password-based authentication applies to passwords regardless of whether they are used in single-factor or multi-factor authentication. Long passwords or passphrases are preferable over shorter passwords. Enforced

composition rules provide marginal security benefits while decreasing usability. However, organizations may choose to establish certain rules for password generation (e.g., minimum character length for long passwords) under certain circumstances and can enforce this requirement in IA-05(01)h. Account recovery can occur, for example, in situations when a password is forgotten. Cryptographically protected passwords include salted one-way cryptographic hashes of passwords. The list of commonly used, compromised, or expected passwords includes passwords obtained from previous breach corpuses, dictionary words, and repetitive or sequential characters. The list includes context-specific words, such as the name of the service, username, and derivatives thereof.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Identification and Authentication Standard. **State:** DIR Security Control Standards Catalog. **Federal:** FIPS 140, 180, 201, 202; NIST SP 800-63-3, 800-73-4, 800-76-2, 800-78-4; NIST IR 7539, 7817, 7849, 7870, 8040; FBI CJIS CSP v5.9	IA-6.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; password policy; procedures addressing authenticator management; system security plan; system design documentation; system configuration settings and associated documentation; password configurations and associated documentation; other relevant documents or records.

Interview: Organizational personnel with authenticator management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers.

Test: Automated mechanisms supporting and/or implementing password-based authenticator management capability.

IA-05(02): PKI-BASED AUTHENTICATION

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The information system

a. For PKI-based authentication:

   1. Enforce authorized access to the corresponding private key; and
   2. Map the authenticated identity to the account of the individual or group; and

b. When public key infrastructure (PKI) is used:

   1. Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and
   2. Implement a local cache of revocation data to support path discovery and validation.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Certificate use must comply with the DFPS Identification and Authentication Standard.

SUPPLEMENTAL GUIDANCE

Public key cryptography is a valid authentication mechanism for individuals, machines, and devices. For PKI solutions, status information for certification paths includes certificate revocation lists or certificate status protocol responses. For PIV cards, certificate validation involves the construction and verification of a certification path to the Common Policy Root trust anchor, which includes certificate policy processing. Implementing a local cache of revocation data to support path discovery and validation also supports system availability in situations where organizations are unable to access revocation information via the network.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Identification and Authentication Standard. **State:** DIR Security Control Standards Catalog. **Federal:** FIPS 140, 180, 201, 202; NIST SP 800-63-3, 800-73-4, 800-76-2, 800-78-4; NIST IR 7539, 7817, 7849, 7870, 8040; FBI CJIS CSP v5.9	IA-3, SC-17.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; procedures addressing authenticator management; system security plan; system design documentation; system configuration settings and associated documentation; PKI certification validation records; PKI certification revocation lists; other relevant documents or records.

Interview: Organizational personnel with PKI-based, authenticator management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers.

Test: Automated mechanisms supporting and/or implementing PKI-based, authenticator management capability.

IA-05(05): CHANGE AUTHENTICATORS PRIOR TO DELIVERY

Priority: P1	
Baseline(s): N/A	Overlay(s): CJIS

CONTROL REQUIREMENTS

For systems processing CJIS data, the following additional Implementation Standard applies:

The organization requires developers/installers of information system components to provide unique authenticators or change default authenticators prior to delivery/installation.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

This control enhancement extends the requirement for organizations to change default authenticators upon information system installation, by requiring developers and/or installers to provide unique authenticators or change default authenticators for system components prior to delivery and/or installation. However, it typically does not apply to the developers of commercial off-the-shelve information technology products. Requirements for unique authenticators can be included in acquisition documents prepared by organizations when procuring information systems or system components.

REFERENCES	RELATED CONTROLS
Federal: FBI CJIS CSP v5.9	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; system security plan; system and services acquisition policy; procedures addressing authenticator management; procedures addressing the integration of security requirements into the acquisition process; acquisition documentation; acquisition contracts for system procurements or services; other relevant documents or records.

Interview: Organizational personnel with authenticator management responsibilities; organizational personnel with information security, acquisition, and contracting responsibilities; system developers.

Test: Automated mechanisms supporting and/or implementing authenticator management capability.

IA-05(06): PROTECTION OF AUTHENTICATORS

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization protects authenticators commensurate with the security category of the information to which use of the authenticator permits access.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - Users must take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and immediately reporting lost or compromised authenticators.

Std.02 - Establish administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators.

SUPPLEMENTAL GUIDANCE

For information systems containing multiple security categories of information without reliable physical or logical separation between categories, authenticators used to grant access to the systems are protected commensurate with the highest security category of information on the systems.

REFERENCES	**RELATED CONTROLS**
Federal: FBI CJIS CSP v5.9	RA-2.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; procedures addressing authenticator management; system security plan; system design documentation; system configuration settings and associated documentation; PKI certification validation records; PKI certification revocation lists; other relevant documents or records.

Interview: Organizational personnel with PKI-based, authenticator management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers.

Test: Automated mechanisms supporting and/or implementing PKI-based, authenticator management capability.

IA-05(07): NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - Never allow credentials to be embedded directly within the application code.

Std.02 - Embedding database credentials within source code is not acceptable.

SUPPLEMENTAL GUIDANCE

Organizations exercise caution in determining whether embedded or stored authenticators are in encrypted or unencrypted form. If authenticators are used in the manner stored, then those representations are considered unencrypted authenticators. This is irrespective of whether that representation is perhaps an encrypted version of something else (e.g., a password).

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Identification and Authentication Standard. **Federal:** FBI CJIS CSP v5.9	RA-2.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; procedures addressing authenticator management; security categorization documentation for the system; security assessments of authenticator protections; risk assessment results; system security plan; other relevant documents or records.

Interview: Organizational personnel with authenticator management responsibilities; organizational personnel implementing and/or maintaining authenticator protections; organizational personnel with information security responsibilities; system/network administrators.

Test: Automated mechanisms supporting and/or implementing authenticator management capability; automated mechanisms protecting authenticators.

IA-05(08): MULTIPLE INFORMATION SYSTEM ACCOUNTS

Priority: P1

Baseline(s): N/A	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization implements defined security safeguards to manage the risk of compromise due to individuals having accounts on multiple information systems.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - Users must take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and immediately reporting lost or compromised authenticators.

Std.02 - Establish administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators.

SUPPLEMENTAL GUIDANCE

Organizations exercise caution in determining whether embedded or stored authenticators are in encrypted or unencrypted form. If authenticators are used in the manner stored, then those representations are considered unencrypted authenticators. This is irrespective of whether that representation is perhaps an encrypted version of something else (e.g., a password).

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Identification and Authentication Standard. **Federal:** FBI CJIS CSP v5.9	PS-6.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; procedures addressing authenticator management; security categorization documentation for the system; security assessments of authenticator protections; risk assessment results; system security plan; other relevant documents or records.

Interview: Organizational personnel with authenticator management responsibilities; organizational personnel implementing and/or maintaining authenticator protections; organizational personnel with information security responsibilities; system/network administrators.

Test: Automated mechanisms supporting and/or implementing authenticator management capability; automated mechanisms protecting authenticators.

IA-05(10) DYNAMIC CREDENTIAL BINDING

Priority: P1

Baseline(s): N/A	Overlay(s): CJIS

CONTROL REQUIREMENTS

The information system dynamically provisions identities.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE
Authentication requires some form of binding between an identity and the authenticator used to confirm the identity. In conventional approaches, this binding is established by pre-provisioning both the identity and the authenticator to the information system. For example, the binding between a username (i.e., identity) and a password (i.e., authenticator) is accomplished by provisioning the identity and authenticator as a pair in the information system. New authentication techniques allow the binding between the identity and the authenticator to be implemented outside an information system. For example, with smartcard credentials, the identity and the authenticator are bound together on the card. Using these credentials, information systems can authenticate identities that have not been pre-provisioned, dynamically provisioning the identity after authentication. In these situations, organizations can anticipate the dynamic provisioning of identities. Preestablished trust relationships and mechanisms with appropriate authorities to validate identities and related credentials are essential.

REFERENCES	RELATED CONTROLS
Federal: FBI CJIS CSP v5.9	AU-16, IA-5.

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Identification and authentication policy; procedures addressing authenticator management; security categorization documentation for the system; security assessments of authenticator protections; risk assessment results; system security plan; other relevant documents or records. Interview: Organizational personnel with authenticator management responsibilities; organizational personnel implementing and/or maintaining authenticator protections; organizational personnel with information security responsibilities; system/network administrators. Test: Automated mechanisms supporting and/or implementing authenticator management capability; automated mechanisms protecting authenticators.

IA-06: AUTHENTICATOR FEEDBACK

Priority: P1	
Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS
The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.
AGENCY IMPLEMENTATION STANDARDS
Std.01 — The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals. [Source: DIR Control Standards Catalog IA-6] Std.02 — All authenticators must be obscured in accordance with the DFPS Identification and Authentication Standard.

SUPPLEMENTAL GUIDANCE

Authentication feedback from systems does not provide information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of systems, such as desktops or notebooks with relatively large monitors, the threat (referred to as shoulder surfing) may be significant. For other types of systems, such as mobile devices with small displays, the threat may be less significant and is balanced against the increased likelihood of typographic input errors due to small keyboards. Thus, the means for obscuring authentication feedback is selected accordingly. Obscuring authentication feedback includes displaying asterisks when users type passwords into input devices or displaying feedback for a very limited time before obscuring it.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Identification and Authentication Standard. **State:** DIR Security Control Standards Catalog. **Federal:** FBI CJIS CSP v5.9	AC-3.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; system security plan; procedures addressing authenticator feedback; system design documentation; system configuration settings and associated documentation; system audit records; other relevant documents or records.

Interview: Organizational personnel with information security responsibilities; system/network administrators; system developers.

Test: Automated mechanisms supporting and/or implementing the obscuring of feedback of authentication information during authentication.

IA-07: CRYPTOGRAPHIC MODULE AUTHENTICATION

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Encryption used by DFPS meets the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module. [Source: DIR Control Standards Catalog IA-7]

Std.02 — Implement encryption algorithms in accordance with SC-13.

SUPPLEMENTAL GUIDANCE	
Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorized to assume the requested role and perform services within that role.	
REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** FIPS 140; FBI CJIS CSP v5.9	AC-3, IA-5, SA-4, SC-12, SC-13.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; system security plan; procedures addressing cryptographic module authentication; system design documentation; system configuration settings and associated documentation; system audit records; other relevant documents or records.

Interview: Organizational personnel with responsibility for cryptographic module authentication; organizational personnel with information security responsibilities; system/network administrators; system developers.

Test: Automated mechanisms supporting and/or implementing cryptographic module authentication.

IA-08: IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)

Priority: P1	
Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

AGENCY IMPLEMENTATION STANDARDS

Std.01 — The information system must uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users). [Source: DIR Control Standards Catalog IA-8]

Std.02 — Each system's identification and authentication mechanisms must comply with the DFPS Identification and Authentication Standard.

SUPPLEMENTAL GUIDANCE

Non-organizational users include system users other than organizational users explicitly covered by IA-02. Non-organizational users are uniquely identified and authenticated for accesses other than those explicitly identified and documented in AC-14. Identification and authentication of non-organizational users accessing federal systems may be required to protect federal, proprietary, or privacy-related information (with exceptions noted for national security systems). Organizations consider many factors—including security, privacy, scalability, and

practicality—when balancing the need to ensure ease of use for access to federal information and systems with the need to protect and adequately mitigate risk.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Identification and Authentication Standard. **State:** DIR Security Control Standards Catalog. **Federal:** OMB A-130; Federal Public Key Infrastructure; FIPS 201; NIST SP 800-63-3, 800-79-2, 800-116; NIST IR 8062; FBI CJIS CSP v5.9	AC-2, AC-6, AC-14, AC-17, AC-18, AU-6, IA-2, IA-4, IA-5, IA-10, IA-11, MA-4, RA-3, SA-4, SC-8.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; system security plan; privacy plan; procedures addressing user identification and authentication; system design documentation; system configuration settings and associated documentation; system audit records; list of system accounts; other relevant documents or records.

Interview: Organizational personnel with system operations responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators; organizational personnel with account management responsibilities.

Test: Automated mechanisms supporting and/or implementing identification and authentication capabilities.

IA-08(02): ACCEPTANCE OF THIRD-PARTY CREDENTIALS

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

For systems processing CJIS data, the following additional Implementation Standard applies:

The information system accepts only FICAM-approved third-party credentials.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

This control enhancement typically applies to organizational information systems that are accessible to the general public, for example, public-facing websites. Third-party credentials are those credentials issued by nonfederal government entities approved by the Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions initiative. Approved third-party credentials meet or exceed the set of minimum federal government-wide technical, security, privacy, and organizational maturity requirements. This allows federal government relying parties to trust such credentials at their approved assurance levels.

REFERENCES	RELATED CONTROLS
Federal: FIPS 201; FBI CJIS CSP v5.9	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; system security plan; privacy plan; procedures addressing user identification and authentication; system design documentation; system configuration settings and associated documentation; system audit records; list of system accounts; other relevant documents or records.

Interview: Organizational personnel with system operations responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators; organizational personnel with account management responsibilities.

Test: Automated mechanisms supporting and/or implementing identification and authentication capabilities.

IA-08(03): USE OF FICAM-APPROVED PRODUCTS

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

This control is withdrawn and incorporated into IA-08(02) but still referenced in the FBI CJIS Security Policy v5.9. Please see IA-08(02).

IA-11: RE-AUTHENTICATION

Priority: P0

Baseline(s): Low, Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

Require users to re-authenticate when circumstances or situations require re-authentication according to the DFPS Identification and Authentication Standard.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

In addition to the re-authentication requirements associated with device locks, organizations may require re-authentication of individuals in certain situations, including when roles, authenticators or credentials change,

when security categories of systems change, when the execution of privileged functions occurs, after a fixed time period, or periodically..

REFERENCES	RELATED CONTROLS
Agency: DFPS Identification and Authentication Standard; DFPS Information Security Policy Manual.	AC-3, AC-11, IA-2, IA-3, IA-4, IA-8.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; procedures addressing user and device re-authentication; system security plan; system design documentation; system configuration settings and associated documentation; list of circumstances or situations requiring re-authentication; system audit records; other relevant documents or records.

Interview: Organizational personnel with system operations responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers; organizational personnel with identification and authentication responsibilities.

Test: Automated mechanisms supporting and/or implementing identification and authentication capabilities.

IA-12: IDENTITY PROOFING

Priority: P0

Baseline(s): Low, Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization:

a. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines;
b. Resolve user identities to a unique individual; and
c. Collect, validate, and verify identity evidence.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Ensure that evidence used for identity proofing complies with requirements as defined in the DFPS Identification and Authentication Standard.

SUPPLEMENTAL GUIDANCE

In addition to the re-authentication requirements associated with device locks, organizations may require re-authentication of individuals in certain situations, including when roles, authenticators or credentials change, when security categories of systems change, when the execution of privileged functions occurs, after a fixed time period, or periodically..

REFERENCES	RELATED CONTROLS

Agency: DFPS Identification and Authentication Standard; DFPS Information Security Policy Manual.	AC-3, AC-11, IA-2, IA-3, IA-4, IA-8.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; procedures addressing identity proofing; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with system operations responsibilities; organizational personnel with information security and privacy responsibilities; legal counsel; system/network administrators; system developers; organizational personnel with identification and authentication responsibilities.

Test: Automated mechanisms supporting and/or implementing identification and authentication capabilities.

IA-12(01): SUPERVISOR AUTHORIZATION

Priority: P0

Baseline(s): Low, Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

Require that the registration process to receive an account for logical access includes supervisor or sponsor authorization.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Ensure that the registration process to receive an account complies with requirements as defined in the DFPS Account Management Policy.

SUPPLEMENTAL GUIDANCE

In addition to the re-authentication requirements associated with device locks, organizations may require re-authentication of individuals in certain situations, including when roles, authenticators or credentials change, when security categories of systems change, when the execution of privileged functions occurs, after a fixed time period, or periodically..

REFERENCES	RELATED CONTROLS
Agency: DFPS Identification and Authentication Standard; DFPS Information Security Policy Manual.	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; procedures addressing identity proofing; system security plan; other relevant documents or records.

Interview: Organizational personnel with system operations responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers; organizational personnel with identification and authentication responsibilities.

Test: Automated mechanisms supporting and/or implementing identification and authentication capabilities.

IA-12(02) IDENTITY EVIDENCE

Priority: P0

Baseline(s): Low, Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

Require evidence of individual identification be presented to the registration authority.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Ensure that the registration process to receive an account complies with requirements as defined in the DFPS Account Management Policy.

Std.02 — DFPS employees, as well as to many DFPS volunteers, interns, contractors, and employees of other state agencies are required to complete a Federal Bureau of Investigations (FBI) fingerprint check to access DFPS information resources. [Source: DFPS Background Checks Handbook]

SUPPLEMENTAL GUIDANCE

Identity evidence, such as documentary evidence or a combination of documents and biometrics reduces the likelihood of individuals using fraudulent identification to establish an identity or at least increases the work factor of potential adversaries. The forms of acceptable evidence are consistent with the risks to the systems, roles, and privileges associated with the user's account.

REFERENCES	RELATED CONTROLS
Agency: DFPS Identification and Authentication Standard; DFPS Information Security Policy **Federal:** FIPS 201; NIST SP 800-63-3, 800-63A, 800-79-2; FBI CJIS CSP v5.9	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; procedures addressing identity proofing; system security plan; other relevant documents or records.

Interview: Organizational personnel with system operations responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers; organizational personnel with identification and authentication responsibilities.

Test: Automated mechanisms supporting and/or implementing identification and authentication capabilities.

IA-12(03): IDENTITY EVIDENCE VALIDATION AND VERIFICATION

Priority: P0

Baseline(s): Low, Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

Require that the presented identity evidence be validated and verified through methods of validation and verification in accordance with the assurance levels defined in the DFPS Identification and Authentication Standard.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Ensure that the registration process to receive an account complies with requirements as defined in the DFPS Account Management Policy.

Std.02 — DFPS employees, as well as to many DFPS volunteers, interns, contractors, and employees of other state agencies are required to complete a Federal Bureau of Investigations (FBI) fingerprint check to access DFPS information resources. [Source: DFPS Background Checks Handbook]

SUPPLEMENTAL GUIDANCE

Identity evidence, such as documentary evidence or a combination of documents and biometrics reduces the likelihood of individuals using fraudulent identification to establish an identity or at least increases the work factor of potential adversaries. The forms of acceptable evidence are consistent with the risks to the systems, roles, and privileges associated with the user's account.

REFERENCES	RELATED CONTROLS
Agency: DFPS Identification and Authentication Standard; DFPS Information Security Policy; DFPS Background Checks Handbook. **Federal:** FIPS 201; NIST SP 800-63-3, 800-63A, 800-79-2; FBI CJIS CSP v5.9	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; procedures addressing identity proofing; system security plan; other relevant documents or records.

Interview: Organizational personnel with system operations responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers; organizational personnel with identification and authentication responsibilities.

Test: Automated mechanisms supporting and/or implementing identification and authentication capabilities.

IA-12(04): IN-PERSON VALIDATION AND VERIFICATION

Priority: P0

Baseline(s): Low, Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

Require that the validation and verification of identity evidence be conducted in person before a designated registration authority.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS employees, as well as to many DFPS volunteers, interns, contractors, and employees of other state agencies are required to complete a Federal Bureau of Investigations (FBI) fingerprint check to access DFPS information resources. [Source: DFPS Background Checks Handbook]

SUPPLEMENTAL GUIDANCE

In-person proofing reduces the likelihood of fraudulent credentials being issued because it requires the physical presence of individuals, the presentation of physical identity documents, and actual face-to-face interactions with designated registration authorities.

REFERENCES	RELATED CONTROLS
Agency: DFPS Identification and Authentication Standard; DFPS Information Security Policy; DFPS Background Checks Handbook. **Federal:** FIPS 201; NIST SP 800-63-3, 800-63A, 800-79-2; FBI CJIS CSP v5.9	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; procedures addressing identity proofing; system security plan; other relevant documents or records.

Interview: Organizational personnel with system operations responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers; organizational personnel with identification and authentication responsibilities.

Test: Automated mechanisms supporting and/or implementing identification and authentication capabilities.

(IR) INCIDENT RESPONSE

DFPS Office of Information Security establishes an operational incident handling capability for DFPS information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities. The DFPS Office of Information Security tracks, documents, and reports incidents to appropriate DFPS and/or authorities.

IR controls are specific to DFPS incident response policies and procedures. This includes incident response training, testing, monitoring, reporting, and response plan. The intended audience for this Control includes but is not limited to all information owners, managers, system administrators, all users of DFPS information resources the DFPS Chief Information Security Officer (CISO) and/or their designee and the Office of Information Security.

IR-01: INCIDENT RESPONSE POLICY AND PROCEDURES

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Develop, document, and disseminate to appropriate personnel:
   1. 1. Organization-level incident response policy that:
      c) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      d) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls;

b. Designate a senior management official as defined in the incident response policy to manage the development, documentation, and dissemination of the incident response policy and procedures; and

c. c. Review and update the current incident response:
   3. Policy every year and following major changes to legislation or security requirements; and
   4. Procedures every year and following major changes to legislation or security requirements.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - Assess the significance of a security incident based on the business impact on the affected resources and the current and potential technical effect of the incident, e.g., loss of revenue, productivity, access to services, reputation, unauthorized disclosure of confidential information, or propagation to other networks. [Source: DIR Control Standards Catalog IR-1]

Std.02 — The DFPS Chief Information Security Officer is responsible for:

a. Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks;

b. Providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities under 1 TAC 202; and

c. Developing and recommending policies and establishing procedures and practices, in cooperation with the agency Information Resources Manager, information-owners and custodians, necessary to ensure the security

of information and information resources against unauthorized or accidental modification, destruction, or disclosure. [Source: 1 TAC 202.21(b)(3, 5, 8)]

Std.03 — The Agency must follow DFPS and State of Texas procedures and guidance in responding to any suspected information security incidents.

a. Identification of information security incidents must be prompted by any suspicious information resource behavior that can be attributed to a suspected or confirmed intentional threat actor.
b. Reporting of information security incidents shall follow the DFPS incident notification matrix.
c. Resolution of information security incidents shall follow guidance provided by DFPS and State of Texas, any outside incident response providers, and industry accepted best practices for information security incident investigation and remediation.

Std.03 — Third-parties must follow the DFPS Contractor Data and System Security Requirements in reporting incidents.

a. The Vendor must notify DFPS Contract Manager and Office of Information Security (infosec@dfps.texas.gov) verbally and in writing of any confirmed or suspected breach of its systems that may affect Sensitive Information within one calendar day after discovery of a breach or of receiving notification of a breach.

SUPPLEMENTAL GUIDANCE

Incident response policy and procedures address the controls in the IR family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of incident response policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations.

Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to incident response policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** OMB A-130; NIST SP 800-12, 800-30, 800-39, 800-50, 800-61, 800-83, 800-100; FBI CJIS CSP v5.9	PM-9, PS-8, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Incident response policy and procedures; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with incident response responsibilities; organizational personnel with information security and privacy responsibilities.

IR-02: INCIDENT RESPONSE TRAINING

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Provide incident response training to system users consistent with assigned roles and responsibilities:
   1. Within 60 days of assuming an incident response role or responsibility or acquiring system access;
   2. When required by system changes; and
   3. Annually thereafter; and

b. Review and update incident response training content annually and following major changes to the environment of operation, including legislation and threats.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - Train personnel in their incident response roles and responsibilities with respect to the information system and provides refresher training at least annually. [Source: DIR Control Standards Catalog IR-2]

Std.02 — Include content on incident identification and reporting in awareness training for all employees and contractors in accordance with AT-02.

Std.03 — Provide role-based training to personnel assigned incident response roles in accordance with AT-03.

Std.04 — Formally track personnel participating in incident response training in accordance with AT-04.

SUPPLEMENTAL GUIDANCE

Incident response training is associated with the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail are included in such training. For example, users may only need to know who to call or how to recognize an incident; system administrators may require additional training on how to handle incidents; and incident responders may receive more specific training on forensics, data collection techniques, reporting, system recovery, and system restoration. Incident response training includes user training in identifying and reporting suspicious activities from external and internal sources. Incident response training for users may be provided as part of AT-02 or AT-03. Events that may precipitate an update to incident response training content include, but are not limited to, incident response plan testing or response to an actual incident (lessons learned), assessment or audit findings, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** OMB M-17-12; NIST SP 800-50; FBI CJIS CSP v5.9	AT-2, AT-3, AT-4, CP-3, IR-3, IR-4, IR-8, IR-9.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Incident response policy; procedures addressing incident response training; incident response training curriculum; incident response training materials; privacy plan; incident response plan; incident response training records; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with incident response training and operational responsibilities; organizational personnel with information security and privacy responsibilities.

IR-02(01): SIMULATED EVENTS

Priority: P1

Baseline(s): High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - Simulated events may include fake phising campaigns targeted toward users; tabletop exercises for incident response staff; and off-site exercises as part of incident response testing.

Std.02 - Document results of training and update training plans and plans of action and milestones (POAMs) accordingly.

SUPPLEMENTAL GUIDANCE

Organizations establish requirements for responding to incidents in incident response plans. Incorporating simulated events into incident response training helps to ensure that personnel understand their individual responsibilities and what specific actions to take in crisis situations.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Phishing Security Awareness Training Policy. **State:** DIR Security Control Standards Catalog. **Federal:** OMB M-17-12; NIST SP 800-50.	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Incident response policy; procedures addressing incident response training; incident response training curriculum; incident response training materials; incident response plan; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with incident response training and operational responsibilities; organizational personnel with information security and privacy responsibilities.

Test: Automated mechanisms that support and/or implement simulated events for incident response training.

IR-02(02): AUTOMATED TRAINING ENVIRONMENTS

Priority: P1

Baseline(s): High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization employs automated mechanisms to provide a more thorough and realistic incident response training environment.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Automated mechanisms can provide a more thorough and realistic incident response training environment. This can be accomplished, for example, by providing more complete coverage of incident response issues, selecting more realistic training scenarios and environments, and stressing the response capability.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Phishing Security Awareness Training Policy. **State:** DIR Security Control Standards Catalog. **Federal:** OMB M-17-12; NIST SP 800-50.	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Incident response policy; procedures addressing incident response training; incident response training curriculum; incident response training materials; incident response plan; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with incident response training and operational responsibilities; organizational personnel with information security and privacy responsibilities.

Test: Automated mechanisms that provide a thorough and realistic incident response training environment.

IR-02(03): BREACH

Priority: P1

Baseline(s): High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization provides incident response training on how to identify and respond to a breach, including the organization's process for reporting a breach.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Ensure that awareness training includes breach awareness and reporting.

SUPPLEMENTAL GUIDANCE

For federal agencies, an incident that involves personally identifiable information is considered a breach. A breach results in the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or a similar occurrence where a person other than an authorized user accesses or potentially accesses personally identifiable information or an authorized user accesses or potentially accesses such information for other than authorized purposes. The incident response training emphasizes the obligation of individuals to report both confirmed and suspected breaches involving information in any medium or form, including paper, oral, and electronic. Incident response training includes tabletop exercises that simulate a breach. See IR-02(01).

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Phishing Security Awareness Training Policy. **State:** DIR Security Control Standards Catalog. **Federal:** OMB M-17-12; NIST SP 800-50.	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Incident response policy; contingency planning policy; procedures addressing incident response testing; procedures addressing contingency plan testing; incident response testing material; incident response

test results; incident response test plan; incident response plan; contingency plan; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with incident response training and operational responsibilities; organizational personnel with information security and privacy responsibilities.

IR-03: INCIDENT RESPONSE TESTING

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization test the effectiveness of the incident response capability for the system at least annually using the following tests: approved tests as identified in the incident response plan.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — The written incident response plan must include provisions for annual testing.

Std.02 — Incident response plans for all new systems must be tested prior to the system's being deployed to an operational state in the production environment.

Std.03 — Major deficiencies discovered as a result of testing must be addressed in accordance with CA-05 to improve existing processes, procedures, and policies.

Std.04 —

a. A formal test need not be conducted if the organization actively exercises its response capability during real incidents.
b. Any response capability not exercised during real incidents must be formally tested.

Std.05 — For cloud service providers, the organization defines tests and/or exercises in accordance with NIST SP 800-61.

Std.06 — For cloud service providers, the organization provides test plans to FedRAMP at least every 365 days. Test plans are approved and accepted by the JAB prior to commencing testing.

SUPPLEMENTAL GUIDANCE

Organizations test incident response capabilities to determine their effectiveness and identify potential weaknesses or deficiencies. Incident response testing includes the use of checklists, walk-through or tabletop exercises, and simulations (parallel or full interrupt).

Incident response testing can include a determination of the effects on organizational operations and assets and individuals due to incident response. The use of qualitative and quantitative data aids in determining the effectiveness of incident response processes.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** OMB M-17-12; NIST SP 800-50; FBI CJIS CSP v5.9	CP-3, CP-4, IR-2, IR-4, IR-8, PM-14.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Incident response policy; contingency planning policy; procedures addressing incident response testing; procedures addressing contingency plan testing; incident response testing material; incident response test results; incident response test plan; incident response plan; contingency plan; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with incident response testing responsibilities; organizational personnel with information security and privacy responsibilities.

IR-03(02): COORDINATION WITH RELATED PLANS

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization coordinate incident response testing with organizational elements responsible for related plans.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Ensure that results of tests are shared with personnel responsible for related plans. Agency-wide full-scale simulations and exercises include personnel responsible for all applicable plans.

SUPPLEMENTAL GUIDANCE

Organizational plans related to incident response testing include business continuity plans, disaster recovery plans, continuity of operations plans, contingency plans, crisis communications plans, critical infrastructure plans, and occupant emergency plans.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** OMB M-17-12; NIST SP 800-84, 800-115.	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Incident response policy; contingency planning policy; procedures addressing incident response testing; incident response testing documentation; incident response plan; business continuity plans; contingency plans; disaster recovery plans; continuity of operations plans; crisis communications plans; critical infrastructure plans; occupant emergency plans; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with incident response testing responsibilities; organizational personnel with responsibilities for testing organizational plans related to incident response testing; organizational personnel with information security and privacy responsibilities.

IR-04: INCIDENT HANDLING

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery;

b. Coordinate incident handling activities with contingency planning activities;

c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and

d. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS must implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. [Source: DIR Control Standards Catalog IR-4]

Std.02 — Ensure that personnel investigating incidents are adequately trained and meet personnel security requirements appropriate to the criticality/sensitivity of the information being processed, stored, and transmitted by the information system.

Std.03 — Maintain appropriate contacts with relevant authorities. Include key law enforcement contacts for reporting security incidents and external third parties authorized to take action against attack sources (for example, internet service providers), and designate a point of contact to review the list at least annually to keep it current. [Source: Hitrust 05.f Contact with Authorities]

Std.04 — Put mechanisms in place to monitor and quantify the types, volumes, and costs of information security incidents. Use the information gained from evaluation of information security incidents to identify recurring or high-impact incidents and update the incident response and recovery strategy. [Source: Hitrust 11.d Learning from Information Security Incidents]

Std.05 — Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented in support of potential legal action in accordance with the rules for evidence in the relevant jurisdiction(s). [Source: Hitrust 11.e Collection of Evidence]

SUPPLEMENTAL GUIDANCE

Organizations recognize that incident response capabilities are dependent on the capabilities of organizational systems and the mission and business processes being supported by those systems. Organizations consider incident response as part of the definition, design, and development of mission and business processes and

systems. Incident-related information can be obtained from a variety of sources, including audit monitoring, physical access monitoring, and network monitoring; user or administrator reports; and reported supply chain events. An effective incident handling capability includes coordination among many organizational entities (e.g., mission or business owners, system owners, authorizing officials, human resources offices, physical security offices, personnel security offices, legal departments, risk executive function, operations personnel, procurement offices). Suspected security incidents include the receipt of suspicious email communications that can contain malicious code. Suspected supply chain incidents include the insertion of counterfeit hardware or malicious code into organizational systems or system components. For federal agencies, an incident that involves personally identifiable information is considered a breach. A breach results in unauthorized disclosure, the loss of control, unauthorized acquisition, compromise, or a similar occurrence where a person other than an authorized user accesses or potentially accesses personally identifiable information or an authorized user accesses or potentially accesses such information for other than authorized purposes.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** Secure Technology Act; 41 CFR 201; OMB M-17-12; NIST SP 800-61, 800-86, 800-101, 800-150, 800-160-2, 800-184; NIST IR 7559; FBI CJIS CSP v5.9	AC-19, AU-6, AU-7, CM-6, CP-2, CP-3, CP-4, IR-2, IR-3, IR-5, IR-6, IR-8, PE-6, PL-2, PM-12, SA-8, SC-5, SC-7, SI-3, SI-4, SI-7.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Incident response policy; contingency planning policy; procedures addressing incident handling; incident response plan; contingency plan; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with incident handling responsibilities; organizational personnel with contingency planning responsibilities; organizational personnel with information security and privacy responsibilities.

Test: Incident handling capability for the organization.

IR-04(01): AUTOMATED INCIDENT HANDLING PROCESSES

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization employs automated mechanisms to support the incident handling process.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Automated mechanisms support the exchange of incident handling information with DFPS Office of Information Security:

a. Information must be provided to DFPS Office of Information Security in a format compliant with DFPS and, if applicable, federal requirements;
b. Incident handling information sources include systems, appliances, devices, services, and applications (including databases);
c. Incident handling information sources that do not support the exchange of information with DFPS Information Security must be documented in the applicable risk assessment and System Security Plan (SSP); and
d. DFPS Office of Information Security-directed incident handling information collection rules/requests (for example, sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.

SUPPLEMENTAL GUIDANCE

Automated mechanisms that support incident handling processes include online incident management systems and tools that support the collection of live response data, full network packet capture, and forensic analysis.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** Secure Technology Act; 41 CFR 201; OMB M-17-12; NIST SP 800-61, 800-86, 800-101, 800-150, 800-160-2, 800-184; NIST IR 7559; FBI CJIS CSP v5.9	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Incident response policy; procedures addressing incident handling; automated mechanisms supporting incident handling; system design documentation; system configuration settings and associated documentation; system audit records; incident response plan; system security plan; other relevant documents or records.

Interview: Organizational personnel with incident handling responsibilities; organizational personnel with information security responsibilities.

Test: Automated mechanisms that support and/or implement the incident handling process.

IR-04(02): DYNAMIC RECONFIGURATION

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization includes dynamic reconfiguration of the information system components as part of the incident response capability.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Dynamic reconfiguration of the information system must be documented in the applicable risk assessment and System Security Plan (SSP).

SUPPLEMENTAL GUIDANCE

Dynamic reconfiguration includes, for example, changes to router rules, access control lists, intrusion detection/prevention system parameters, and filter rules for firewalls and gateways. Organizations perform dynamic reconfiguration of information systems, for example, to stop attacks, to misdirect attackers, and to isolate components of systems, thus limiting the extent of the damage from breaches or compromises. Organizations include time frames for achieving the reconfiguration of information systems in the definition of the reconfiguration capability, considering the potential need for rapid response in order to effectively address sophisticated cyber threats.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** FBI CJIS CSP v5.9	AC-2, AC-4, CM-2.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Incident response policy; procedures addressing incident handling; automated mechanisms supporting incident handling; list of system components to be dynamically reconfigured as part of incident response capability; system design documentation; system configuration settings and associated documentation; system audit records; incident response plan; system security plan; other relevant documents or records.

Interview: Organizational personnel with incident handling responsibilities; organizational personnel with information security responsibilities.

Test: Automated mechanisms that support and/or implement dynamic reconfiguration of components as part of incident response.

IR-04(03): CONTINUITY OF OPERATIONS

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization identifies incidents and responses to classes of incident to ensure continuation of organizational missions and business functions. Classes of incident are based on attack vector (e.g. attack via external media, the web, improper system use, loss of equipment) and serve to further define specific handling procedures.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Ensure that incident response training and actions include multiple possible attack vectors.

SUPPLEMENTAL GUIDANCE

Classes of incidents include malfunctions due to design or implementation errors and omissions, targeted malicious attacks, and untargeted malicious attacks. Incident response actions include orderly system degradation, system shutdown, fall back to manual mode or activation of alternative technology whereby the system operates differently, employing deceptive measures, alternate information flows, or operating in a mode that is reserved for when systems are under attack. Organizations consider whether continuity of operations requirements during an incident conflict with the capability to automatically disable the system as specified as part of IR-4(5).

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** FBI CJIS CSP v5.9	AC-2, AC-4, CM-2.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Incident response policy; procedures addressing incident handling; incident response plan; privacy plan; list of classes of incidents; list of appropriate incident response actions; system security plan; other relevant documents or records.

Interview: Organizational personnel with incident handling responsibilities; organizational personnel with information security responsibilities.

Test: Automated mechanisms that support and/or implement continuity of operations.

IR-04(04): INFORMATION CORRELATION

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Ensure that system-specific incident information is reported and correlated across business areas and across events.

SUPPLEMENTAL GUIDANCE

Sometimes the nature of a threat event, for example, a hostile cyber-attack, is such that it can only be observed by bringing together information from different sources including various reports and reporting procedures established by organizations.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** Secure Technology Act; 41 CFR 201; OMB M-17-12; NIST SP 800-61, 800-86, 800-101, 800-150, 800-160-2, 800-184; NIST IR 7559;FBI CJIS CSP v5.9	AC-2, AC-4, CM-2.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Incident response policy; procedures addressing incident handling; incident response plan; privacy plan; automated mechanisms supporting incident and event correlation; system design documentation; system configuration settings and associated documentation; system security plan; privacy plan; incident management correlation logs; event management correlation logs; security information and event management logs; incident management correlation reports; event management correlation reports; security information and event management reports; audit records; other relevant documents or records.

Interview: Organizational personnel with incident handling responsibilities; organizational personnel with information security and privacy responsibilities; organizational personnel with whom incident information and individual incident responses are to be correlated.

Test: Organizational processes for correlating incident information and individual incident responses; automated mechanisms that support and or implement the correlation of incident response information with individual incident responses.

IR-05: INCIDENT MONITORING

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization tracks and documents information system security incidents.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Track and document information system security incidents on an ongoing basis. [Source: DIR Control Standards Catalog IR-5]

Std.02 — Monitor logs per CA-07. Log, report, investigate, and respond to all verified signs of incidents in accordance with the system-specific incident response plan.

Std.03 — Forward information system security and privacy incident and breach information:

a. In accordance with reporting requirements defined under the current DFPS Incident Response Plan; and
b. Provide incident and breach information in a format compliant with DFPS, state, and, if applicable, federal (for example, Continuous Diagnostics and Mitigation) requirements.

Std.04 — Signifigant information security incidents are tracked in the Texas Department of Information Resources eGRC platform (SPECTRIM).

Std.05 — All documentation obtained from an information security incident is kept in an electronic storage platform with appropriate access controls limiting access to authorized personnel.

SUPPLEMENTAL GUIDANCE

Documenting incidents includes maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics as well as evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources, including network monitoring, incident reports, incident response teams, user complaints, supply chain partners, audit monitoring, physical access monitoring, and user and administrator reports. IR-04 provides information on the types of incidents that are appropriate for monitoring.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** Secure Technology Act; NIST SP 800-61;FBI CJIS CSP v5.9	AU-6, AU-7, IR-4, IR-6, IR-8, PE-6, PM-5, SC-5, SC-7, SI-3, SI-4, SI-7.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Incident response policy; procedures addressing incident monitoring; incident response records and documentation; incident response plan; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with incident monitoring responsibilities; organizational personnel with information security and privacy responsibilities.

Test: Incident monitoring capability for the organization; automated mechanisms supporting and/or implementing tracking and documenting of system security incidents.

IR-05(01): AUTOMATED TRACKING / DATA COLLECTION / ANALYSIS

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Monitor and quantify the types, volumes, and costs of information security incidents. [Source: Hitrust 11.d Learning from Information Security Incidents]

Std.02 — Ensure that incident records are restricted to only authorized personnel.

SUPPLEMENTAL GUIDANCE

Automated mechanisms for tracking incidents and collecting and analyzing incident information include Computer Incident Response Centers or other electronic databases of incidents and network monitoring devices.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP 800-61; FBI CJIS CSP v5.9	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Incident response policy; procedures addressing incident monitoring; incident response records and documentation; system security plan; incident response plan; other relevant documents or records.

Interview: Organizational personnel with incident monitoring responsibilities; organizational personnel with information security responsibilities.

Test: Incident monitoring capability for the organization; automated mechanisms supporting and/or implementing tracking and documenting of system security incidents.

IR-06: INCIDENT REPORTING

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Require personnel to report suspected incidents to the organizational incident response capability immediately upon discovery; and
b. Report incident information to appropriate individuals in accordance with the organization incident response policy and procedures.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Security incidents must be promptly reported to immediate supervisors and the DFPS Office of Information Security Office. Security incidents that require timely reporting to the Department of Information Resources (DIR) include those events that are assessed to:

a. Propagate to other state systems;
b. Result in criminal violations that shall be reported to law enforcement; or
c. Involve the unauthorized disclosure or modification of confidential information, e.g., sensitive personal information as defined in Sec. 521.002(a)(2), Business and Commerce Code, and other applicable laws that may require public notification. [Source: DIR Control Standards Catalog IR-6]

Std.02 — If the security incident is assessed to involve suspected criminal activity (e.g., violations of Chapters 33, Penal Code (Computer Crimes) or Chapter 33A, Penal Code(Telecommunications Crimes)), the security incident shall be investigated, reported, and documented in a manner that restores operation promptly while meeting the legal requirements for handling of evidence. [Source: DIR Control Standards Catalog IR-6]

Std.03 — Summary reports of security-related events shall be sent to DIR on a monthly basis no later than nine calendar days after the end of the month. DFPS shall submit summary security incident reports in the form and manner specified by DIR. Supporting vendors or other third parties that report security incident information to DFPS shall submit such reports to DFPS in the form and manner specified by DIR, unless otherwise directed by DFPS. [Source: DIR Control Standards Catalog IR-6]

Std.04 — The DFPS Chief Information Security Officer, or designee must report Urgent Incident Reports to the Department of Information Resources. [Source: 1 TAC 202.23(b)]

Std.05 — DFPS, as a state agency that owns, licenses, or maintains computerized data that includes sensitive personal information, confidential information, or information the disclosure of which is regulated by law shall, in the event of a breach or suspected breach of system security or an unauthorized exposure of that information:

a. Comply with the notification requirements of Section 521.053, Business & Commerce Code, to the same extent as a person who conducts business in this state; and
b. Not later than 24 hours after the discovery of the breach, suspected breach, or unauthorized exposure, notify:
    1) The Department of Information Resources, including the chief information security officer; or
    2) If the breach, suspected breach, or unauthorized exposure involves election data, the secretary of state. [Source: TX Govt. Code 2054.1125(b)]

Std.06 — Not later than the 10th business day after the date of the eradication, closure, and recovery from a breach, suspected breach, or unauthorized exposure, DFPS shall notify the Department of Information Resources, including the chief information security officer, of the details of the event and include in the notification an analysis of the cause of the event. [Source: TX Govt. Code 2054.1125(c)]

SUPPLEMENTAL GUIDANCE

The intent of this control is to address both specific incident reporting requirements within an organization and the formal incident reporting requirements for federal agencies and their subordinate organizations. Suspected security incidents include, for example, the receipt of suspicious email communications that can potentially contain malicious code. The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Current federal policy requires that all federal agencies (unless specifically exempted from such requirements) report security incidents to the United States Computer Emergency Readiness Team (US-CERT) within specified time frames designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy.	CM-6, CP-2, IR-4, IR-5, IR-8, IR-9.

State: 1 TAC 202.23(b); TX Govt. Code 2054.1125; DIR Security Control Standards Catalog. **Federal:** Secure Technology Act; 41 CFR 201; US-CERT Federal Incident Notification Guidelines; NIST SP 800-61; FBI CJIS CSP v5.9	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Incident response policy; procedures addressing incident monitoring; incident response records and documentation; system security plan; incident response plan; other relevant documents or records.

Interview: Organizational personnel with incident monitoring responsibilities; organizational personnel with information security responsibilities.

Test: Incident monitoring capability for the organization; automated mechanisms supporting and/or implementing tracking and documenting of system security incidents.

IR-06(01): AUTOMATED REPORTING

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization employs automated mechanisms to assist in the reporting of security incidents.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Employ secure automated mechanisms to support the incident reporting process in accordance with the incident response plan.

SUPPLEMENTAL GUIDANCE

The recipients of incident reports are specified in IR-06b. Automated reporting mechanisms include email, posting on websites (with automatic updates), and automated incident response tools and programs.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** Secure Technology Act; 41 CFR 201; US-CERT Federal Incident Notification Guidelines; NIST SP 800-61; FBI CJIS CSP v5.9	IR-7.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Incident response policy; procedures addressing incident reporting; automated mechanisms supporting incident reporting; system design documentation; system configuration settings and associated documentation; incident response plan; system security plan; other relevant documents or records.

Interview: Organizational personnel with incident reporting responsibilities; organizational personnel with information security responsibilities.

Test: Organizational processes for incident reporting; automated mechanisms supporting and/or implementing reporting of security incidents.

IR-06(02): VULNERABILITIES RELATED TO INCIDENTS

Priority: P1

Baseline(s): N/A	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization reports information system vulnerabilities associated with reported security incidents in accordance with IR-6

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Ensure reports of confirmed security incidents on DFPS information system document the exploited vulnerabilities in accordance with IR-6

SUPPLEMENTAL GUIDANCE

The recipients of incident reports are specified in IR-06b. Automated reporting mechanisms include email, posting on websites (with automatic updates), and automated incident response tools and programs.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** Secure Technology Act; 41 CFR 201; US-CERT Federal Incident Notification Guidelines; NIST SP 800-61; FBI CJIS CSP v5.9	IR-7.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Incident response policy; procedures addressing incident reporting; automated mechanisms supporting incident reporting; system design documentation; system configuration settings and associated documentation; incident response plan; system security plan; other relevant documents or records.

Interview: Organizational personnel with incident reporting responsibilities; organizational personnel with information security responsibilities.

Test: Organizational processes for incident reporting; automated mechanisms supporting and/or implementing reporting of security incidents.

IR-06(03): SUPPLY CHAIN COORDINATION

Priority: P1

Baseline(s): N/A	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization provides security incident information to other organizations involved in the supply chain for information systems or information system components related to the incident.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Ensure that information is reviewed and approved for sending based on agreements with the suppliers. (Any escalation of or exception from this reporting should be clearly defined in the agreement.) Ensure that incident reporting data is adequately protected for transmission and received by approved individuals only. [Source: SP 800-161]

SUPPLEMENTAL GUIDANCE

Organizations involved in supply chain activities include product developers, system integrators, manufacturers, packagers, assemblers, distributors, vendors, and resellers. Entities that provide supply chain governance include the Federal Acquisition Security Council (FASC). Supply chain incidents include compromises or breaches that involve information technology products, system components, development processes or personnel, distribution processes, or warehousing facilities. Organizations determine the appropriate information to share and consider the value gained from informing external organizations about supply chain incidents, including the ability to improve processes or to identify the root cause of an incident.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** Secure Technology Act; 41 CFR 201; US-CERT Federal Incident Notification Guidelines; NIST SP 800-61;	SR-8.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Incident response policy; procedures addressing supply chain coordination and supply chain risk information sharing with the Federal Acquisition Security Council; acquisition policy; acquisition contracts;

service-level agreements; incident response plan; supply chain risk management plan; system security plan; plans of other organizations involved in supply chain activities; other relevant documents or records.

Interview: Organizational personnel with incident reporting responsibilities; organizational personnel with information security responsibilities; organizational personnel with supply chain risk management responsibilities; organization personnel with acquisition responsibilities.

Test: Organizational processes for incident reporting; organizational processes for supply chain risk information sharing; automated mechanisms supporting and/or implementing reporting of incident information involved in the supply chain.

IR-07: INCIDENT RESPONSE ASSISTANCE

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS must provide an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource is an integral part of DFPS incident response capability. [Source: DIR Control Standards Catalog IR-7]

Std.02 — Ensure basic awareness training (see AT-02) includes content on identification and reporting of potential incidents.

Std.03 — Provide monitored communication methods (for example, e-mail boxes) for reporting potential incidents.

SUPPLEMENTAL GUIDANCE

Incident response support resources provided by organizations include help desks, assistance groups, automated ticketing systems to open and track incident response tickets, and access to forensics services or consumer redress services, when required.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; NIST IR 7559; FBI CJIS CSP v5.9	AT-2, AT-3, IR-4, IR-6, IR-8, PM-22, PM-26, SA-9, SI-18.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Incident response policy; procedures addressing incident response assistance; incident response plan; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with incident response assistance and support responsibilities; organizational personnel with access to incident response support and assistance capability; organizational personnel with information security and privacy responsibilities.

Test: Organizational processes for incident response assistance; automated mechanisms supporting and/or implementing incident response assistance.

IR-07(01): AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION / SUPPORT

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization employs automated mechanisms to increase the availability of incident response-related information and support.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Provide automated mechanisms for tracking the status of potential incidents.

Std.02 — When incident response activities may affect users, where feasible provide near real time announcements including incident response-related information on websites, ticketing systems, or by e-mail.

SUPPLEMENTAL GUIDANCE

Automated mechanisms can provide a push and/or pull capability for users to obtain incident response assistance. For example, individuals might have access to a website to query the assistance capability, or conversely, the assistance capability may have the ability to proactively send information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; NIST IR 7559; FBI CJIS CSP v5.9	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Incident response policy; procedures addressing incident response assistance; automated mechanisms supporting incident response support and assistance; system design documentation; system configuration settings and associated documentation; incident response plan; system security plan; other relevant documents or records.

Interview: Organizational personnel with incident response support and assistance responsibilities; organizational personnel with access to incident response support and assistance capability; organizational personnel with information security responsibilities.

Test: Organizational processes for incident response assistance; automated mechanisms supporting and/or implementing an increase in the availability of incident response information and support.

IR-07(02): COORDINATION WITH EXTERNAL PROVIDERS

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization:

a. Establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability; and
b. Identifies organizational incident response team members to the external providers.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - Incident handling information that support the exchange of information with DFPS Office of Information Security must be documented in the applicable risk assessment and System Security Plan (SSP) and communicated with external providers.

SUPPLEMENTAL GUIDANCE

Automated mechanisms can provide a push and/or pull capability for users to obtain incident response assistance. For example, individuals might have access to a website to query the assistance capability, or conversely, the assistance capability may have the ability to proactively send information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; NIST IR 7559; FBI CJIS CSP v5.9	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Incident response policy; procedures addressing incident response assistance; incident response plan; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with incident response support and assistance responsibilities; external providers of system protection capability; organizational personnel with information security and privacy responsibilities.

IR-08: INCIDENT RESPONSE PLAN

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Develops an incident response plan that:
   1. Provides the organization with a roadmap for implementing its incident response capability;
   2. Describes the structure and organization of the incident response capability;
   3. Provides a high-level approach for how the incident response capability fits into the overall organization;
   4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
   5. Defines reportable incidents;
   6. Provides metrics for measuring the incident response capability within the organization;
   7. Defines the resources and management support needed to effectively maintain and mature an incident response capability;
   8. Addresses the sharing of incident information;
   9. Is reviewed and approved by the DFPS Chief Information Security Officer (CISO) (or equivalent) on an annual basis and when significant changes to the plan are made; and
   10. Explicitly designates responsibility for incident response to entities, personnel, or roles as defined within the incident response policy.
b. Distribute copies of the incident response plan to entities, personnel, or roles as identified within the incident response policy;
c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing;
d. Communicate incident response plan changes to entities, personnel, or roles as identified within the incident response policy; and
e. Protect the incident response plan from unauthorized disclosure and modification.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS must have an incident management policy that describes the requirements for dealing with computer security incidents including prevention, detection, response, remediation, and reporting. [Source: DIR Control Standards Catalog IR-8]

SUPPLEMENTAL GUIDANCE

It is important that organizations develop and implement a coordinated approach to incident response. Organizational mission and business functions determine the structure of incident response capabilities. As part of the incident response capabilities, organizations consider the coordination and sharing of information with external organizations, including external service providers and other organizations involved in the supply chain. For incidents involving personally identifiable information (i.e., breaches), include a process to determine whether notice to oversight organizations or affected individuals is appropriate and provide that notice accordingly.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130, M-17-12; NIST SP 800-61; FBI CJIS CSP v5.9	AC-2, CP-2, CP-4, IR-4, IR-7, IR-9, PE-6, PL-2, SA-15, SI-12, SR-8.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Incident response policy; procedures addressing incident response planning; incident response plan; system security plan; privacy plan; records of incident response plan reviews and approvals; other relevant documents or records.

Interview: Organizational personnel with incident response planning responsibilities; organizational personnel with information security and privacy responsibilities.

Test: Organizational incident response plan and related organizational processes.

IR-08(01): BREACHES

Priority: P1

Baseline(s): Privacy	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

Include the following in the Incident Response Plan for breaches involving personally identifiable information:

a. A process to determine if notice to individuals or other organizations, including oversight organizations, is needed;
b. An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and
c. Identification of applicable privacy requirements.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Where DFPS computerized data includes sensitive personal information (SPI), DFPS will disclose any breach of system security, after discovering or receiving notification of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made without unreasonable delay and in each case not later than the 60th day after the date on which the person determines that the breach occurred, except as provided by Subsection (d) or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system. [Source: Bus. & Comm. 521.053(b)]

SUPPLEMENTAL GUIDANCE

Organizations may be required by law, regulation, or policy to follow specific procedures relating to breaches, including notice to individuals, affected organizations, and oversight bodies; standards of harm; and mitigation or other specific requirements.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** Bus. & Comm. 521.053; DIR Security Control Standards Catalog.	PT-1, PT-2, PT-3, PT-4, PT-5, PT-7.

Federal: OMB A-130, M-17-12; NIST SP 800-61.	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Incident response policy; procedures addressing incident response planning; incident response plan; system security plan; privacy plan; records of incident response plan reviews and approvals; other relevant documents or records.

Interview: Organizational personnel with incident response planning responsibilities; organizational personnel with information security and privacy responsibilities.

Test: Organizational incident response plan and related organizational processes.

IR-09: INFORMATION SPILLAGE RESPONSE

Priority: P0

Baseline(s): N/A	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization responds to information spills by:

a. Identifying the specific information involved in the information system contamination;
b. Alerting incident response personnel (as defined in the SSP and the incident response plan [See IR-06]) of the information spill using a method of communication not associated with the spill;
c. Isolating the contaminated information system or system component;
d. Eradicating the information from the contaminated information system or component;
e. Identifying other information systems or system components that may have been subsequently contaminated; and
f. Performing required response actions as in the system incident response plan.

AGENCY IMPLEMENTATION STANDARDS

Std.01 —DFPS responds to information spills by requiring personnel to report suspected incidents as defined in IR-06.

SUPPLEMENTAL GUIDANCE

Information spillage refers to instances where information is placed on systems that are not authorized to process such information. Information spills occur when information that is thought to be a certain classification or impact level is transmitted to a system and subsequently is determined to be of a higher classification or impact level. At that point, corrective action is required. The nature of the response is based on the classification or impact level of the spilled information, the security capabilities of the system, the specific nature of the contaminated storage media, and the access authorizations of individuals with authorized access to the contaminated system. The methods used to communicate information about the spill after the fact do not involve methods directly associated with the actual spill to minimize the risk of further spreading the contamination before such contamination is isolated and eradicated.

REFERENCES	**RELATED CONTROLS**

Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130, M-17-12; NIST SP 800-61.	CP-2, IR-6, PM-26, PM-27, PT-2, PT-3, PT-7, RA-7.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Incident response policy; procedures addressing information spillage; incident response plan; system security plan; records of information spillage alerts/notifications; list of personnel who should receive alerts of information spillage; list of actions to be performed regarding information spillage; other relevant documents or records.

Interview: Organizational personnel with incident response responsibilities; organizational personnel with information security responsibilities.

Test: Organizational processes for information spillage response; automated mechanisms supporting and/or implementing information spillage response actions and related communications.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130, M-17-12; NIST SP 800-61.	CP-2, IR-6, PM-26, PM-27, PT-2, PT-3, PT-7, RA-7.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Incident response policy; procedures addressing information spillage; incident response plan; system security plan; records of information spillage alerts/notifications; list of personnel who should receive alerts of information spillage; list of actions to be performed regarding information spillage; other relevant documents or records.

Interview: Organizational personnel with incident response responsibilities; organizational personnel with information security responsibilities.

Test: Organizational processes for information spillage response; automated mechanisms supporting and/or implementing information spillage response actions and related communications.

(MA) MAINTENANCE

DFPS requires that periodic and timely maintenance on DFPS information systems occur and effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance are in place.

The intended audience for this Control includes, but is not limited to, information resource owners and custodians. The information resource owner, or their designee, is responsible for ensuring that the

maintenance management measures described in this Control family are implemented by personnel with maintenance management responsibilities (e.g. system/network administrators, information security analyst, etc.).

MA-01: SYSTEM MAINTENANCE POLICY AND PROCEDURES	
Priority: P1	
Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Develop, document, and disseminate to appropriate personnel:
   1. Organization-level maintenance policy that:
      a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls;
b. Designate a senior management official as defined in the maintenance policy to manage the development, documentation, and dissemination of the maintenance policy and procedures; and
c. Review and update the current maintenance:
   1. Policy every year and following major changes to legislation or security requirements; and
   2. Procedures every year and following major changes to legislation or security requirements.

AGENCY IMPLEMENTATION STANDARDS

Std.01 —DFPS must have a policy that addresses system maintenance controls. [Source: DIR Control Standards Catalog MA-1]

The DFPS Information Security Officer shall be responsible for:

a. Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks;
b. Providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities under 1 TAC 202; and
c. Developing and recommending policies and establishing procedures and practices, in cooperation with the agency Information Resources Manager, information-owners and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, or disclosure. [Source: 1 TAC 202.21(b)(3, 5, 8)]

SUPPLEMENTAL GUIDANCE

Maintenance policy and procedures address the controls in the MA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of maintenance policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations.

Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the

individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to maintenance policy and procedures assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130, M-17-12; NIST SP 800-61; FBI CJIS CSP v5.9	PM-9, PS-8, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Maintenance policy and procedures; system security plan; privacy plan; organizational risk management strategy; other relevant documents or record.

Interview: Organizational personnel with maintenance responsibilities; organizational personnel with information security and privacy responsibilities.

MA-02: CONTROLLED MAINTENANCE

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements;
b. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location;
c. Require that system owners or other authorized personnel as identified in the System Security Plan (SSP) explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement;
d. Sanitize equipment to remove the following information from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement: all DFPS data;
e. Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and
f. Include the following information in organizational maintenance records: maintenance- related information as defined in Std.02.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Schedule, perform, document, and review records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements. [Source: DIR Control Standards Catalog MA-2]

Std.02 — Records of maintenance activity must be maintained in organization maintenance records or system maintenance logs and must include:

a. Date and time of maintenance;
b. Name(s) of individual(s) performing maintenance;
c. Name of escort, if necessary;
d. Description of maintenance performed; and
e. List of equipment removed or replaced, including identification numbers if applicable.

Std.03 — Where feasible, employ automated mechanisms to schedule and conduct maintenance as required, and to create current, correct, and complete records of all maintenance actions whether needed, scheduled, in process, or performed.

Std.04 — Following maintenance or repair, check to ensure maintenance ports have been disabled and security features re-enabled.

SUPPLEMENTAL GUIDANCE

Controlling system maintenance addresses the information security aspects of the system maintenance program and applies to all types of maintenance to system components conducted by local or nonlocal entities. Maintenance includes peripherals such as scanners, copiers, and printers. Information necessary for creating effective maintenance records includes the date and time of maintenance, a description of the maintenance performed, names of the individuals or group performing the maintenance, name of the escort, and system components or equipment that are removed or replaced. Organizations consider supply chain-related risks associated with replacement components for systems.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; NIST IR 8023; FBI CJIS CSP v5.9	CM-2, CM-3, CM-4, CM-5, CM-8, MA-4, MP-6, PE-16, SI-2, SR-3, SR-4, SR-11.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Maintenance policy; procedures addressing controlled system maintenance; maintenance records; manufacturer/vendor maintenance specifications; equipment sanitization records; media sanitization records; system security plan; other relevant documents or records.

Interview: Organizational personnel with system maintenance responsibilities; organizational personnel with information security responsibilities; organizational personnel responsible for media sanitization; system/network administrators.

Test: Maintenance policy; procedures addressing controlled system maintenance; maintenance records; manufacturer/vendor maintenance specifications; equipment sanitization records; media sanitization records; system security plan; other relevant documents or records.

MA-02(02): AUTOMATED MAINTENANCE ACTIVITIES

Priority: P1	
Baseline(s): High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization:

a. Schedule, conduct, and document maintenance, repair, and replacement actions for the system using automated mechanisms as identified in applicable System Security Plans (SSPs); and

b. Produce up-to date, accurate, and complete records of all maintenance, repair, and replacement actions requested, scheduled, in process, and completed.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

The use of automated mechanisms to manage and control system maintenance programs and activities helps to ensure the generation of timely, accurate, complete, and consistent maintenance records.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; NIST IR 8023.	MA-3.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Maintenance policy; procedures addressing controlled system maintenance; automated mechanisms supporting system maintenance activities; system configuration settings and associated documentation; maintenance records; system security plan; other relevant documents or records.

Interview: Organizational personnel with system maintenance responsibilities; organizational personnel with information security responsibilities; system/network administrators.

Test: Automated mechanisms supporting and/or implementing controlled maintenance; automated mechanisms supporting and/or implementing production of records of maintenance and repair actions.

MA-03: MAINTENANCE TOOLS

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Approve, control, and monitor the use of system maintenance tools; and
b. Review previously approved system maintenance tools at least annually as part of the review of the System Security Plan (SSP).

AGENCY IMPLEMENTATION STANDARDS

Std.01 —

a. Document approved maintenance tools in System Security Plans.

b. For each approved tool, list any system maintenance ports, services, and protocols that must be disabled according to configuration standards but are required by the tool.

Std.02 — Ensure that maintenance tools are included in maintenance schedules (see MA- 02).

SUPPLEMENTAL GUIDANCE

Approving, controlling, monitoring, and reviewing maintenance tools address security-related issues associated with maintenance tools that are not within system authorization boundaries and are used specifically for diagnostic and repair actions on organizational systems. Organizations have flexibility in determining roles for the approval of maintenance tools and how that approval is documented. A periodic review of maintenance tools facilitates the withdrawal of approval for outdated, unsupported, irrelevant, or no-longer- used tools. Maintenance tools can include hardware, software, and firmware items and may be pre-installed, brought in with maintenance personnel on media, cloud-based, or downloaded from a website. Such tools can be vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and subsequently into systems.

Maintenance tools can include hardware and software diagnostic test equipment and packet sniffers. The hardware and software components that support maintenance and are a part of the system (including the software implementing utilities such as "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch) are not addressed by maintenance tools.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: NIST SP 800-88; FBI CJIS CSP v5.9	MA-2, PE-16.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Maintenance policy; procedures addressing system maintenance tools; system maintenance tools and associated documentation; maintenance records; system security plan; other relevant documents or records.

Interview: Organizational personnel with system maintenance responsibilities; organizational personnel with information security responsibilities.

Test: Organizational processes for approving, controlling, and monitoring maintenance tools; automated mechanisms supporting and/or implementing approval, control, and/or monitoring of maintenance tools.

MA-03(01): INSPECT TOOLS

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Ensure that maintenance tools are inspected as defined by policy (see MA-01).

Std.02 — Explicitly authorize, track, and audit any removal of maintenance tools. [Source: SP 800-161]

SUPPLEMENTAL GUIDANCE

Maintenance tools can be directly brought into a facility by maintenance personnel or downloaded from a vendor's website. If, upon inspection of the maintenance tools, organizations determine that the tools have been modified in an improper manner or the tools contain malicious code, the incident is handled consistent with organizational policies and procedures for incident handling.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: NIST SP 800-88; FBI CJIS CSP v5.9	SI-7.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Maintenance policy; procedures addressing system maintenance tools; system maintenance tools and associated documentation; maintenance tool inspection records; maintenance records; system security plan; other relevant documents or records.

Interview: Organizational personnel with system maintenance responsibilities; organizational personnel with information security responsibilities.

Test: Organizational processes for inspecting maintenance tools; automated mechanisms supporting and/or implementing inspection of maintenance tools.

MA-03(02): INSPECT MEDIA

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Ensure that media containing maintenance diagonstic tools/programs are inspected as defined by policy (see MA-01).

Std.02 — Explicitly authorize, track, and audit any removal of maintenance tools. [Source: SP 800-161]

SUPPLEMENTAL GUIDANCE

If, upon inspection of media containing maintenance diagnostic and test programs, organizations determine that the media contain malicious code, the incident is handled consistent with organizational incident handling policies and procedures.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: NIST SP 800-88; FBI CJIS CSP v5.9	SI-3.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Maintenance policy; procedures addressing system maintenance tools; system maintenance tools and associated documentation; maintenance records; equipment sanitization records; media sanitization records; exemptions for equipment removal; system security plan; other relevant documents or records.

Interview: Organizational personnel with system maintenance responsibilities; organizational personnel with information security responsibilities; organizational personnel responsible for media sanitization.

Test: Organizational process for preventing unauthorized removal of information; automated mechanisms supporting media sanitization or destruction of equipment; automated mechanisms supporting verification of media sanitization

MA-03(03): PREVENT UNAUTHORIZED REMOVAL

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization prevents the unauthorized removal of maintenance equipment containing organizational information by:

a. Verifying that there is no organizational information contained on the equipment;
b. Sanitizing or destroying the equipment;

c. Retaining the equipment within the facility; or
d. Obtaining an exemption from personnel or roles as identified in the System Security Plan (SSP) explicitly authorizing removal of the equipment from the facility.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Ensure all maintenance equipment with the capability of retaining information is sanitized as required by MP-06 before removal from organization-controlled facilities; or, if sanitization is not feasible, retain or destroy the equipment unless authorized to release.

Std.02 — Explicitly authorize, track, and audit any removal of maintenance tools. [Source: SP 800-161]

a. Once tools are allowed access to an organization/information system, they should remain the property/asset of the information system owner and tracked if removed and used elsewhere in the organization. Maintenance tools either currently in use or in storage should not be allowed to leave the organization's premises until they are properly vetted for removal. [Source: SP 800-161]

SUPPLEMENTAL GUIDANCE

Organizational information includes all information owned by organizations and any information provided to organizations for which the organizations serve as information stewards.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: NIST SP 800-88; FBI CJIS CSP v5.9	MP-6.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Maintenance policy; procedures addressing system maintenance tools; system maintenance tools and associated documentation; maintenance records; system security plan; other relevant documents or records.

Interview: Organizational personnel with system maintenance responsibilities; organizational personnel with information security responsibilities.

Test: Organizational process for inspecting media for malicious code; automated mechanisms supporting and/or implementing inspection of media used for maintenance.

MA-04: NONLOCAL MAINTENANCE

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Approve and monitor nonlocal maintenance and diagnostic activities;

b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;
c. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions;
d. Maintain records for nonlocal maintenance and diagnostic activities; and
e. Terminate session and network connections when nonlocal maintenance is completed.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Authorize, monitor, and control any remotely executed maintenance and diagnostic activities, if employed. [Source: DIR Control Standards Catalog MA-4]

Std.02 — When maintenance is to be conducted by a third party, personnel with appropriate authorizations and technical competence, as identified in the System Security Plan (SSP), must:

a. Set up the required connection features;
b. Provide assistance to the third party as required during the session;
c. Monitor the process in real-time;
d. Verify the completion of the maintenance;
e. Verify that all temporarily enabled ports, services, accesses, protocols, and permissions are disabled; and
f. Verify the session termination.

Std.03 — Password-based authentication is permissible for use during remote maintenance only if passwords are changed following each remote maintenance service.

Std.04 — Media used during remote maintenance must be sanitized in accordance with NIST SP 800-88.

Std.05 — Review records in accordance with AU-06.

SUPPLEMENTAL GUIDANCE

Nonlocal maintenance and diagnostic activities are conducted by individuals who communicate through either an external or internal network. Local maintenance and diagnostic activities are carried out by individuals who are physically present at the system location and not communicating across a network connection. Authentication techniques used to establish nonlocal maintenance and diagnostic sessions reflect the network access requirements in IA-02. Strong authentication requires authenticators that are resistant to replay attacks and employ multi-factor authentication. Strong authenticators include PKI where certificates are stored on a token protected by a password, passphrase, or biometric. Enforcing requirements in MA-04 is accomplished, in part, by other controls. SP 800-63B provides additional guidance on strong authentication and authenticators.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FIPS 140, 197, 201; NIST SP 800-63-3, 800-88; FBI CJIS CSP v5.9	AC-2, AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-4, IA-5, IA-8, MA-2, MA-5, PL-2, SC-7, SC-10.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Maintenance policy; procedures addressing nonlocal system maintenance; remote access policy; remote access procedures; system design documentation; system configuration settings and associated documentation; maintenance records; records of remote access; diagnostic records; system security plan; other relevant documents or records.

Interview: Organizational personnel with system maintenance responsibilities; organizational personnel with information security responsibilities; system/network administrators.

Test: Organizational processes for managing nonlocal maintenance; automated mechanisms implementing, supporting, and/or managing nonlocal maintenance; automated mechanisms for strong authentication of nonlocal maintenance diagnostic sessions; automated mechanisms for terminating nonlocal maintenance sessions and network connections.

MA-04(04): COMPARABLE SECURITY AND SANITIZATION

Priority: P1

Baseline(s): High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization:

a. Requires that nonlocal maintenance and diagnostic services be performed from an information system that implements a security capability comparable to the capability implemented on the system being serviced; or
b. Removes the component to be serviced from the information system and prior to nonlocal maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software) before reconnecting the component to the information system.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Ensure that contracts, Memorandums of Understanding (MOUs) and statements of work (SOWs) include requirements for security controls.

Std.02 — Sanitize components in accordance with MP-06(03).

SUPPLEMENTAL GUIDANCE

Comparable security capability on information systems, diagnostic tools, and equipment providing maintenance services implies that the implemented security controls on those systems, tools, and equipment are at least as comprehensive as the controls on the information system being serviced.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FIPS 140, 197, 201; NIST SP 800-63-3, 800-88.	MP-6, SI-3, SI-7.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Maintenance policy; procedures addressing nonlocal system maintenance; service provider contracts and/or service-level agreements; maintenance records; inspection records; audit records; equipment sanitization records; media sanitization records; system security plan; other relevant documents or records.

Interview: Organizational personnel with system maintenance responsibilities; system maintenance provider; organizational personnel with information security responsibilities; organizational personnel responsible for media sanitization; system/network administrators.

Test: Organizational processes for comparable security and sanitization for nonlocal maintenance; organizational processes for the removal, sanitization, and inspection of components serviced via nonlocal maintenance; automated mechanisms supporting and/or implementing component sanitization and inspection.

MA-04(06): CRYPTOGRAPHIC PROTECTION

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

For systems processing CJIS data, the following additional Implementation Standard applies:

The information system implements cryptographic mechanisms to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Encrypting the communications channel when maintenance is performed remotely protects user credentials, sensitive information such as personally identifiable information (PII), and other data as it travels "across the wire."

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FIPS 140, 197, 201; NIST SP 800-63-3, 800-88.	SC-8, SC-12, SC-13.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Maintenance policy; procedures addressing nonlocal system maintenance; system design documentation; system configuration settings and associated documentation; cryptographic mechanisms protecting nonlocal maintenance activities; maintenance records; diagnostic records; audit records; system security plan; other relevant documents or record.

Interview: Organizational personnel with system maintenance responsibilities; network engineers; organizational personnel with information security responsibilities; system/network administrators.

Test: Cryptographic mechanisms protecting nonlocal maintenance and diagnostic communications.

MA-04(07): DISCONNECT VERIFICATION

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

For systems processing CJIS data, the following additional Implementation Standard applies:

The information system implements remote disconnect verification at the termination of nonlocal maintenance and diagnostic sessions.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Remote disconnect verification ensures that remote connections from nonlocal maintenance sessions have been terminated and are no longer available for use.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FIPS 140, 197, 201; NIST SP 800-63-3, 800-88.	AC-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Maintenance policy; procedures addressing nonlocal system maintenance; system design documentation; system configuration settings and associated documentation; cryptographic mechanisms protecting nonlocal maintenance activities; maintenance records; diagnostic records; audit records; system security plan; other relevant documents or records.

Interview: Organizational personnel with system maintenance responsibilities; network engineers; organizational personnel with information security responsibilities; system/network administrators.

Test: Automated mechanisms implementing remote disconnect verifications of terminated nonlocal maintenance and diagnostic session.

MA-05: MAINTENANCE PERSONNEL

Priority: P1	
Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel;
b. Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations; and
c. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Allow only authorized personnel to perform maintenance on the information system. [Source: DIR Control Standards Catalog MA-5]

Std.02 — Before allowing third-party maintenance personnel access to systems, verify that those personnel:

a. Have been validated to meet personnel requirements in accordance with PS-07;
b. Individually sign a confidentiality agreement or non-disclosure agreement (NDA);
c. Provide valid identification;
d. Are authorized to perform work on the specific system(s); and
e. Are expected, whether or not an escort is required.

Std.04 — Equipment is maintained in accordance with the supplier's recommended service intervals and specifications. Only authorized maintenance personnel should carry out repairs and service equipment. Appropriate controls should be implemented when equipment is scheduled for maintenance (e.g., authorization levels) taking into account whether this maintenance is performed by personnel on site or external to the organization. [Source: Hitrust CSF 08.j Equipment Maintenance]

SUPPLEMENTAL GUIDANCE

Maintenance personnel refers to individuals who perform hardware or software maintenance on organizational systems, while PE-02 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems. Technical competence of supervising individuals relates to the maintenance performed on the systems, while having required access authorizations refers to maintenance on and near the systems. Individuals not previously identified as authorized maintenance personnel—such as information technology manufacturers, vendors, systems integrators, and consultants—may require privileged access to organizational systems, such as when they are required to conduct maintenance activities with little or no notice. Based on organizational assessments of risk, organizations may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for very limited time periods.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FBI CJIS CSP v5.9	AC-2, AC-3, AC-5, AC-6, IA-2, IA-8, MA-4, MP-2, PE-2, PE-3, PS-7, RA-3.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Maintenance policy; procedures addressing maintenance personnel; service provider contracts; service-level agreements; list of authorized personnel; maintenance records; access control records; system security plan; other relevant documents or records.

Interview: Organizational personnel with system maintenance responsibilities; organizational personnel with information security responsibilities.

Test: Organizational processes for authorizing and managing maintenance personnel; automated mechanisms supporting and/or implementing authorization of maintenance personnel.

MA-05(01): INDIVIDUALS WITHOUT APPROPRIATE ACCESS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Implement procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements:

   1. Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; and

   2. Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and

b. Develop and implement alternate controls as specified in the System Security Plan (SSP) in the event a system component cannot be sanitized, removed, or disconnected from the system.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Procedures for individuals who lack appropriate security clearances or who are not U.S. citizens are intended to deny visual and electronic access to classified or controlled unclassified information contained on organizational systems. Procedures for the use of maintenance personnel can be documented in security plans for the systems.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog.	MP-6, PL-2.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Maintenance policy; procedures addressing maintenance personnel; system media protection policy; physical and environmental protection policy; list of maintenance personnel requiring escort/supervision; maintenance records; access control records; system security plan; other relevant documents or records.

Interview: Organizational personnel with system maintenance responsibilities; organizational personnel with personnel security responsibilities; organizational personnel with physical access control responsibilities; organizational personnel with information security responsibilities; organizational personnel responsible for media sanitization; system/network administrators.

Test: Organizational processes for managing maintenance personnel without appropriate access; automated mechanisms supporting and/or implementing alternative security safeguards; automated mechanisms supporting and/or implementing information storage component sanitization.

MA-05(04): FOREIGN NATIONALS

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

For systems processing CJIS data, the following additional Implementation Standard applies:

The organization ensures that non-escorted personnel performing maintenance activities not directly associated with the information system but in the physical proximity of the system, have required access authorization.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Personnel performing maintenance activities in other capacities not directly related to the information system include, for example, physical plant personnel and janitorial personnel.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog.	PS-3.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Maintenance policy; procedures addressing maintenance personnel; system media protection policy; access control policy and procedures; physical and environmental protection policy and procedures; maintenance records; access control records; access authorizations; system security plan; other relevant documents or records.

Interview: Organizational personnel with system maintenance responsibilities; organizational personnel with personnel security responsibilities; organizational personnel with physical access control responsibilities; organizational personnel with information security responsibilities.

MA-06: TIMELY MAINTENANCE

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization obtains maintenance support and/or spare parts for system components as defined in contingency plans within time periods defined in contingency plans of failure.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — For information systems and system components not identified in contingency plans (including systems not hosted on the infrastructure platform), obtain support or replacement according to procurement guidelines.

SUPPLEMENTAL GUIDANCE

Organizations specify the system components that result in increased risk to organizational operations and assets, individuals, other organizations, or the Nation when the functionality provided by those components is not operational. Organizational actions to obtain maintenance support include having appropriate contracts in place.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog.	CM-8, CP-2, CP-7, RA-7, SA-15, SI-13, SR-2, SR-3, SR-4.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Maintenance policy; procedures addressing system maintenance; service provider contracts; service-level agreements; inventory and availability of spare parts; system security plan; other relevant documents or records.

Interview: Organizational personnel with system maintenance responsibilities; organizational personnel with acquisition responsibilities; organizational personnel with information security responsibilities; system/network administrators.

Test: Organizational processes for ensuring timely maintenance.

(MP) MEDIA PROTECTION

DFPS requires the protection of digital and non-digital information system media, limiting access to information on information system media to authorized users, and sanitizing or destroying information system media before disposal or released for reuse.

The Media Protection control family includes controls specific to access, marking, storage, transport policies, sanitization, and defined media use. The intended audience for this Control includes but is not limited to all information owners, managers, system administrators, and all users of DFPS information resources (i.e. full-time and contracted staff).

MP-01: MEDIA PROTECTION POLICY AND PROCEDURES

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Develop, document, and disseminate to appropriate personnel:

   1. Organization-level media protection policy that:
      a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls;

b. Designate a senior management official as defined in the media protection policy to manage the development, documentation, and dissemination of the media protection policy and procedures; and

c. Review and update the current media protection:
   1. Policy every two (2) years and following major changes to legislation or security requirements; and
   2. Procedures every two (2) years and following major changes to legislation or security requirements.

AGENCY IMPLEMENTATION STANDARDS

Std.01 —DFPS must have a policy that addresses media protection controls. [Source: DIR Control Standards Catalog MP-1]

Std.02 — The DFPS Chief Information Security Officer (CISO) shall be responsible for:

a. Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks;
b. Providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities under 1 TAC 202; and
c. Developing and recommending policies and establishing procedures and practices, in cooperation with the agency Information Resources Manager, information-owners and custodians, necessary to ensure the security

of information and information resources against unauthorized or accidental modification, destruction, or disclosure. [Source: 1 TAC 202.21(b)(3, 5, 8)]

SUPPLEMENTAL GUIDANCE

Media protection policy and procedures address the controls in the MP family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of media protection policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations.

Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to media protection policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; NIST SP 800-12, 800-30, 800-39, 800-100; FBI CJIS CSP v5.9	PM-9, PS-8, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Media protection policy and procedures; organizational risk management strategy; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with media protection responsibilities; organizational personnel with information security and privacy responsibilities.

MP-02: MEDIA ACCESS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization restricts access to system media, whether digital or non-digital, that contains Sensitive, Confidential or Controlled data to only those personnel the Information Owner has determined need to access the data.

AGENCY IMPLEMENTATION STANDARDS

Std.01 —DFPS must restrict access to information system media to authorized individuals. [Source: DIR Control Standards Catalog MP-2]

Std.02 — The Information Owner or his or her designated representative(s) are responsible for approving access to information resources and periodically reviewing access lists based on documented risk management decisions. [Source: 1 TAC 202.22(1)(B)]

SUPPLEMENTAL GUIDANCE

System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), compact discs, and digital versatile discs. Non-digital media includes paper and microfilm. Denying access to patient medical records in a community hospital unless the individuals seeking access to such records are authorized healthcare providers is an example of restricting access to non-digital media. Limiting access to the design specifications stored on compact discs in the media library to individuals on the system development team is an example of restricting access to digital media.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** 1 TAC 202.22(1)(B); DIR Security Control Standards Catalog **Federal**: OMB A-130; FIPS 199; NIST SP 800-111; FBI CJIS CSP v5.9	AC-19, AU-9, CP-2, CP-9, CP-10, MA-5, MP-4, MP-6, PE-2, PE-3, SC-12, SC-13, SC-34, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Organizational personnel with system media protection responsibilities; organizational personnel with information security responsibilities; system/network administrator,

Interview: Organizational processes for restricting information media; automated mechanisms supporting and/or implementing media access restrictions.

MP-03: MEDIA MARKING

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and

b. Exempt digital and non-digital media classified as Public from marking if the media remain within DFPS-owned or managed facilities.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Classify all DFPS data as specified in PM-05(01).

Std.02 — Mark all media that contains information that is not Public. [Source: DIR Data Classification Template]

Std.03 — All media marking must follow DFPS media protection policy and procedures.

SUPPLEMENTAL GUIDANCE

Security marking refers to the application or use of human-readable security attributes. Digital media includes diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), flash drives, compact discs, and digital versatile discs. Non- digital media includes paper and microfilm. Controlled unclassified information is defined by the National Archives and Records Administration along with the appropriate safeguarding and dissemination requirements for such information and is codified in 32 CFR 2002. Security markings are generally not required for media that contains information determined by organizations to be in the public domain or to be publicly releasable. Some organizations may require markings for public information indicating that the information is publicly releasable. System media marking reflects applicable laws, executive orders, directives, policies, regulations, standards, and guidelines.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: 32 CFR 2002; EO 13556; FIPS 199; FBI CJIS CSP v5.9	AC-16, CP-9, MP-5, PE-22, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System media protection policy; procedures addressing media marking; physical and environmental protection policy and procedures; list of system media marking security attributes; designated controlled areas; system security plan; other relevant documents or records.

Interview: Organizational personnel with system media protection and marking responsibilities; organizational personnel with information security responsibilities.

Test: Organizational processes for marking information media; automated mechanisms supporting and/or implementing media marking.

MP-04: MEDIA STORAGE

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Physically control and securely store system media, whether digital or non-digital, that contains Sensitive, Confidential, or Regulated data within areas where access is not restricted only to personnel authorized to access the media; and

b. Protect system media types defined in MP-04a until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — All DFPS media storage must comply with MP-07.

SUPPLEMENTAL GUIDANCE

System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), compact discs, and digital versatile discs. Non-digital media includes paper and microfilm. Physically controlling stored media includes conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the library, and maintaining accountability for stored media. Secure storage includes a locked drawer, desk, or cabinet or a controlled media library. The type of media storage is commensurate with the security category or classification of the information on the media. Controlled areas are spaces that provide physical and procedural controls to meet the requirements established for protecting information and systems. Fewer controls may be needed for media that contains information determined to be in the public domain, publicly releasable, or have limited adverse impacts on organizations, operations, or individuals if accessed by other than authorized personnel. In these situations, physical access controls provide adequate protection.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FIPS 199; NIST SP 800-56A, 800-56B, 800-56C, 800-57-1, 800-57-2, 800-57-3, 800-111; FBI CJIS CSP v5.9	AC-19, CP-2, CP-6, CP-9, CP-10, MP-2, MP-7, PE-3, PL-2, SC-12, SC-13, SC-28, SC-34, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System media protection policy; procedures addressing media storage; physical and environmental protection policy and procedures; access control policy and procedures; system media; designated controlled areas; system security plan; other relevant documents or records.

Interview: Organizational personnel with system media protection and marking responsibilities; organizational personnel with information security responsibilities.

Test: Organizational processes for storing information media; automated mechanisms supporting and/or implementing secure media storage/media protection.

MP-05: MEDIA TRANSPORT

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Protect and control digital and non-digital media containing DFPS Sensitive, Confidential, or Controlled data during transport outside of controlled areas using methods outlined in Stds.02 & 03;

b. Maintain accountability for system media during transport outside of controlled areas;

c. Document activities associated with the transport of system media; and

d. Restrict the activities associated with the transport of system media to authorized personnel.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Permit only authorized personnel to perform activities associated with transport of media, and maintain records to document pickup, receipt, transfer, and delivery.

Std.02 — Media Security in Transport

a. For digital media, use encryption in accordance with SC-08 and SC-13 to secure the data while in transport.
b. Use tamper-evident packaging to secure the data while in transport.

Std.03 — Transport Method Requirements

a. If hand carried, use a securable container transported by authorized personnel.
b. If shipped, utilize a trackable receipt by a commercial carrier and require a signature for delivery.

Std.04 — All DFPS media being transported must comply with MP-03 and MP-07.

SUPPLEMENTAL GUIDANCE

System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state and magnetic), compact discs, and digital versatile discs. Non-digital media includes microfilm and paper. Controlled areas are spaces for which organizations provide physical or procedural controls to meet requirements established for protecting information and systems. Controls to protect media during transport include cryptography and locked containers. Cryptographic mechanisms can provide confidentiality and integrity protections depending on the mechanisms implemented. Activities associated with media transport include releasing media for transport, ensuring that media enters the appropriate transport processes, and the actual transport. Authorized transport and courier personnel may include individuals external to the organization. Maintaining accountability of media during transport includes restricting transport activities to authorized personnel and tracking and/or obtaining records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering. Organizations establish documentation requirements for activities associated with the transport of system media in accordance with organizational assessments of risk. Organizations maintain the flexibility to define record-keeping methods for the different types of media transport as part of a system of transport-related records.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FIPS 199; NIST SP 800-60-1, 800-60-2; FBI CJIS CSP v5.9	AC-7, AC-19, CP-2, CP-9, MP-3, MP-4, PE-16, PL-2, SC-12, SC-13, SC-28, SC-34.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System media protection policy; procedures addressing media storage; physical and environmental protection policy and procedures; access control policy and procedures; authorized personnel list; system media; designated controlled areas; system security plan; other relevant documents or records.

Interview: Organizational personnel with system media protection and storage responsibilities; organizational personnel with information security responsibilities; system/network administrators.

Test: Organizational processes for storing information media; automated mechanisms supporting and/or implementing media storage/media protection.

MP-05(03): CUSTODIANS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization employs an identified custodian during transport of information system media outside of controlled areas.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Identified custodians provide organizations with specific points of contact during the media transport process and facilitate individual accountability. Custodial responsibilities can be transferred from one individual to another as long as an unambiguous custodian is identified at all times.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FIPS 199; NIST SP 800-60-1, 800-60-2; FBI CJIS CSP v5.9	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; system media transport records; audit records; system security plan; other relevant documents or records.

Interview: Organizational personnel with system media transport responsibilities; organizational personnel with information security responsibilities.

Test: Organizational processes for identifying and employing a custodian to transport media outside of controlled areas.

MP-05(04): CRYPTOGRAPHIC PROTECTION

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

This control is withdrawn and incorporated into SC-28(01) but still referenced in the FBI CJIS Security Policy v5.9. Please see SC-28(01).

MP-06: MEDIA SANITIZATION

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization:

a. Sanitize all digital or non-digital systems or storage media that contains DFPS data prior to disposal, release out of organizational control, or release for reuse using sanitization techniques outlined in Stds.01-10; and

b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Prior to the sale or transfer of data processing equipment, to other than another Texas state agency or agent of the state, DFPS shall assess whether to remove data from any associated storage device. [Source: DIR Controls Standard Catalog MP-6]

Std.02 — Electronic state records shall be destroyed in accordance with Sec. 441.185, Government Code. If the record retention period applicable for an electronic state record has not expired at the time the record is removed from data process equipment, DFPS shall retain a hard copy or other electronic copy of the record for the required retention period. [Source: DIR Controls Standard Catalog MP-6]

Std.03 — If it is possible that restricted personal information, confidential information, mission critical information, intellectual property, or licensed software is contained on the storage device, the storage device should be sanitized or the storage device should be removed and destroyed. Additional information on sanitization tools and methods of destruction (that comply with the Department of Defense 5220.22-M standard)

are provided in the "Sale or Transfer of Computers and Software" guidelines available at http://www.dir.texas.gov. [Source: DIR Controls Standard Catalog MP-6]

Std.04 — Keep a record/form (electronic or hard copy) documenting the removal and completion of the sanitization process with the following information:

a. Date;

b. Description of the item(s) and serial number(s);

c. Inventory number(s);

d. The process and sanitization tools used to remove the data or method of destruction; and

e. The name and address of the organization the equipment was transferred

Std.05 — A state record may not be destroyed if any litigation, claim, negotiation, audit, open records request, administrative review, or other action involving the record is initiated before the expiration of a retention period for the record set by the commission or in the approved records retention schedule of the agency until the completion of the action and the resolution of all issues that arise from the action, or until the expiration of the retention period, whichever is later. [Source: TX Govt. Code 441.187(b)]

Std.06 — Ensure that an electronic state record scheduled for disposition is disposed of in a manner that ensures protection of confidential information. [Source: 13 TAC 6.97(b)]

Std.07 — Establish and implement procedures that address the disposition of electronic state records by staff in accordance with its certified records retention schedule as well as secure destruction requirements from the Department of Information Resources, including identifying and disposing of transitory information. [Source: 13 TAC 6.97(c)]

Std.08 — For any equipment not owned by DFPS, the Agency shall permanently remove data from data processing equipment before disposing of or otherwise transferring the equipment to a person who is not a state agency or other agent of the state. [Source: TX Govt. Code 2054.130(a)]

Std.09 — Sanitize equipment, including removing all labels, markings, and activity logs, degaussing, overwriting, or destroying media, in accordance with the guidance in and/or NIST SP 800-88r1 Guidelines for Media Sanitization.

Std.10 — Test sanitization equipment and procedures at least annually to ensure correct performance.

SUPPLEMENTAL GUIDANCE

Media sanitization applies to all digital and non-digital system media subject to disposal or reuse, whether or not the media is considered removable. Examples include digital media in scanners, copiers, printers, notebook computers, workstations, network components, mobile devices, and non-digital media (e.g., paper and microfilm). The sanitization process removes information from system media such that the information cannot be retrieved or reconstructed. Sanitization techniques—including clearing, purging, cryptographic erase, de-identification of personally identifiable information, and destruction—prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Organizations determine the appropriate sanitization methods, recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization. Organizations use discretion on the employment of approved sanitization techniques and procedures for media that contains information deemed to be in the public domain or publicly releasable or information deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes destruction, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections or words in a manner equivalent in effectiveness to removing them from the document. NSA standards and policies control the sanitization process for media that contains classified information. NARA policies control the sanitization process for controlled unclassified information.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** TX Govt. Code 441.187(b), TX Govt. Code 2054.130; 13 TAC 6.97; DIR Security Control Standards Catalog. **Federal**: 32 CFR 2002; OMB A-130; NARA CUI Registry; FIPS 199; NIST SP 800-60-1, 800-60-2, 800-88, 800-124; NIST IR 8023; NSA Media Destruction Guidance; FBI CJIS CSP v5.9	AC-3, AC-7, AU-11, MA-2, MA-3, MA-4, MA-5, PM-22, SI-12, SI-18, SI-19, SR-11.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System media protection policy; procedures addressing media sanitization and disposal; applicable federal standards and policies addressing media sanitization policy; media sanitization records; system audit records; system design documentation; records retention and disposition policy; records retention and disposition procedures; system configuration settings and associated documentation; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with media sanitization responsibilities; organizational personnel with records retention and disposition responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators.

Test: Organizational processes for media sanitization; automated mechanisms supporting and/or implementing media sanitization.

MP-06(01): REVIEW / APPROVE / TRACK / DOCUMENT / VERIFY

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization reviews, approves, tracks, documents, and verifies media sanitization and disposal actions.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS shall permanently remove data from data processing equipment before disposing of or otherwise transferring the equipment to a person who is not a state agency or other agent of the state. [Source: TX Govt. Code 2054.130(a)]

Std.02 – For systems processing CJIS data, the following additional Implementation Standard applies:

a. FBI CJIS CSP Section 5.8.3 describes the requirements for agencies to maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies must sanitize (electronically overwrite the data at least three times) or degauss electronic media prior to disposal or release for reuse by unauthorized individuals.

b. The sanitization or destruction needs to be witnessed or carried out only by authorized personnel. Inoperable electronic media must be destroyed (cut up, shredded, etc.)

a. FBI CJIS CSP Section 5.8.4 describes the requirements for physical media to be securely disposed of when no longer required, using established formal procedures. Physical media must be destroyed by shredding or incineration. This disposal or destruction needs to be witnessed or carried out only by authorized personnel.

SUPPLEMENTAL GUIDANCE

Organizations review and approve media to be sanitized to ensure compliance with records retention policies. Tracking and documenting actions include listing personnel who reviewed and approved sanitization and disposal actions, types of media sanitized, files stored on the media, sanitization methods used, date and time of the sanitization actions, personnel who performed the sanitization, verification actions taken and personnel who performed the verification, and the disposal actions taken. Organizations verify that the sanitization of the media was effective prior to disposal

DIR rules for implementation for TX Govt. Code 2054.130(a) includes rules that: specify the types of data processing equipment covered by the section, including computer hard drives and other memory components; explain the acceptable methods for removal of data; and adopt appropriate forms for use by state agencies in documenting the removal process, including forms for documenting completion of the process. [Source: TX Govt. Code 2054.130(b)(1, 2, 3)]

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** TX Govt. Code 2054.130; DIR Security Control Standards Catalog. **Federal**: 32 CFR 2002; OMB A-130; NARA CUI Registry; FIPS 199; NIST SP 800-60-1, 800-60-2, 800-88, 800-124; NIST IR 8023; NSA Media Destruction Guidance; FBI CJIS CSP v5.9	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System media protection policy; procedures addressing media sanitization and disposal; records retention and disposition policy; records retention and disposition procedures; media sanitization and disposal records; review records for media sanitization and disposal actions; approvals for media sanitization and disposal actions; tracking records; verification records; system audit records; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with system media sanitization and disposal responsibilities; organizational personnel with records retention and disposition responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators.

Test: Organizational processes for media sanitization; automated mechanisms supporting and/or implementing media sanitization; automated mechanisms supporting and/or implementing verification of media sanitization.

MP-06(02): EQUIPMENT TESTING

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization tests sanitization equipment and procedures annually to verify that the intended sanitization is being achieved.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Testing of sanitization equipment and procedures may be conducted by qualified and authorized external entities, including federal agencies or external service providers.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** TX Govt. Code 2054.130; DIR Security Control Standards Catalog. **Federal**: 32 CFR 2002; OMB A-130; NARA CUI Registry; FIPS 199; NIST SP 800-60-1, 800-60-2, 800-88, 800-124; NIST IR 8023; NSA Media Destruction Guidance; FBI CJIS CSP v5.9	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System media protection policy; procedures addressing media sanitization and disposal; procedures addressing testing of media sanitization equipment; results of media sanitization equipment and procedures testing; system audit records; records retention and disposition policy; records retention and disposition procedures; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with system media sanitization responsibilities; organizational personnel with records retention and disposition responsibilities; organizational personnel with information security and privacy responsibilities.

Test: Organizational processes for media sanitization; automated mechanisms supporting and/or implementing media sanitization; automated mechanisms supporting and/or implementing media sanitization procedures; sanitization equipment.

MP-06(03): NONDESTRUCTIVE TECHNIQUES

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the information system under the following circumstances: Circumstances as defined in Std.01.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Sanitize portable devices:

a. Upon initial receipt;
b. b. Following any external maintenance or release from organizational control;
c. After any suspected or confirmed event involving the device, if disposal is not warranted; and
d. Prior to release for reuse.

SUPPLEMENTAL GUIDANCE

Portable storage devices include external or removable hard disk drives (e.g., solid state, magnetic), optical discs, magnetic or optical tapes, flash memory devices, flash memory cards, and other external or removable disks. Portable storage devices can be obtained from untrustworthy sources and contain malicious code that can be inserted into or transferred to organizational systems through USB ports or other entry portals. While scanning storage devices is recommended, sanitization provides additional assurance that such devices are free of malicious code. Organizations consider nondestructive sanitization of portable storage devices when the devices are purchased from manufacturers or vendors prior to initial use or when organizations cannot maintain a positive chain of custody for the devices.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** TX Govt. Code 2054.130; DIR Security Control Standards Catalog. **Federal**: 32 CFR 2002; OMB A-130; NARA CUI Registry; FIPS 199; NIST SP 800-60-1, 800-60-2, 800-88, 800-124; NIST IR 8023; NSA Media Destruction Guidance; FBI CJIS CSP v5.9	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System media protection policy; procedures addressing media sanitization and disposal; information on portable storage devices for the system; list of circumstances requiring sanitization of portable storage devices; media sanitization records; audit records; system security plan; other relevant documents or records.

Interview: Organizational personnel with system media sanitization responsibilities; organizational personnel with information security responsibilities.

Test: Organizational processes for media sanitization of portable storage devices; automated mechanisms supporting and/or implementing media sanitization.

MP-07: MEDIA USE

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Restrict the use of digital and non-digital media on systems containing DFPS Sensitive, Confidential or Controlled data using implementation requirements outlined in Stds.02 & 03; and
b. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS must restrict the use of mobile devices with information storage capability, based on documented risk management decisions. [Source: DIR Controls Standard Catalog MP-7].

Std.02 —

a. Digital media cannot be used to store DFPS Sensitive, Confidential or Controlled data unless all the requirements below are followed.

   The digital media must be:

   1. Encrypted in accordance with SC-28(01);
   2. Marked in accordance with MP-03;
   3. Stored when not in use in accordance with MP-04;
   4. Transported in accordance with MP-05;
   5. Disposed of in accordance with MP-06.

b. Non-digital media cannot be used to store DFPS Sensitive, Confidential or Controlled data unless all the requirements below are followed.

   The non-digital media must be:

   1. Marked in accordance with MP-03;
   2. Stored when not in use in accordance with MP-04;
   3. Transported in accordance with MP-05;
   4. Disposed of in accordance with MP-06.

Std.03 — Personally owned digital media should not be used to store DFPS Sensitive, Confidential or Controlled data, unless previously authorized by the DFPS Office of Information Security.

SUPPLEMENTAL GUIDANCE

System media includes both digital and non-digital media. Digital media includes diskettes, magnetic tapes, flash drives, compact discs, digital versatile discs, and removable hard disk drives. Non-digital media includes paper and microfilm. Media use protections also apply to mobile devices with information storage capabilities. In contrast to MP-02, which restricts user access to media, MP-07 restricts the use of certain types of media on systems, for example, restricting or prohibiting the use of flash drives or external hard disk drives.

Organizations use technical and nontechnical controls to restrict the use of system media. Organizations may restrict the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports or disabling or removing the ability to insert, read, or write to such devices. Organizations may also limit the use of portable storage devices to only approved devices, including devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned. Finally, organizations may restrict the use of portable storage devices based on the type of device, such as by prohibiting the use of writeable, portable storage devices and implementing this restriction by disabling or removing the capability to write to such devices. Requiring identifiable owners for storage devices reduces the risk of using such devices by allowing organizations to assign responsibility for addressing known vulnerabilities in the devices.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Acceptable Use Policy; DFPS Data Loss Prevention (DLP) Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FIPS 199; NIST SP 800-111; FBI CJIS CSP v5.9	AC-19, AC-20, PL-4, PM-12, SC-34, SC-41.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System media protection policy; system use policy; procedures addressing media usage restrictions; rules of behavior; system design documentation; system configuration settings and associated documentation; audit records; system security plan; other relevant documents or records.

Interview: Organizational personnel with system media use responsibilities; organizational personnel with information security responsibilities; system/network administrators.

Test: Organizational processes for media use; automated mechanisms restricting or prohibiting use of system media on systems or system components.

(PE) PHYSICAL AND ENVIRONMENTAL PROTECTION CONTROLS

DFPS coordinates with Texas Facilities Commission (TFC) and/or other owning facility management organizations to limit physical access to information systems, equipment, and the respective operating environments to authorized individuals.

The Physical and Environmental Protection control family is implemented to protect systems, buildings, and related supporting infrastructure against physical threats. These controls include physical access authorizations, monitoring, visitor records, emergency shutoff, power, lighting, fire protection, and water damage protection.

The intended audience for this Control includes, but is not limited to, information resource owners and custodians. The information resource owner, or their designee, is responsible for ensuring that the physical and environmental management measures described in this Control family are implemented by personnel with maintenance management responsibilities (e.g. system/network administrators, information security analyst, etc.).

PE-01: PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Develop, document, and disseminate to appropriate personnel:
   1. Organization-level physical and environmental protection policy that:

a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls;

b. Designate a senior management official as defined in the physical and environmental protection policy to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; and
c. Review and update the current physical and environmental protection:
   1. Policy every two (2) years and following major changes to legislation or security requirements; and
   2. Procedures every two (2) years and following major changes to legislation or security requirements.

AGENCY IMPLEMENTATION STANDARDS

Std.01 —DFPS Commissioner or their designated representative(s) shall document and manage physical access to mission critical information resources facilities to ensure the protection of information resources from unlawful or unauthorized access, use, modification or destruction. [Source: DIR Control Standards Catalog PE-1]

Std.02 — The DFPS Chief Information Security Officer shall be responsible for:

a. Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks;
b. Providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities under 1 TAC 202; and
c. Developing and recommending policies and establishing procedures and practices, in cooperation with the agency Information Resources Manager, information-owners and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, or disclosure. [Source: 1 TAC 202.21(b)(3, 5, 8)]

SUPPLEMENTAL GUIDANCE

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PE family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: NIST SP 800-12, 800-30, 800-39, 800-100; FBI CJIS CSP v5.9	AT-3, PM-9, PS-8, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Physical and environmental protection policy and procedures; system security plan; privacy plan; organizational risk management strategy; other relevant documents or records.

Interview: Organizational personnel with physical and environmental protection responsibilities; organizational personnel with information security and privacy responsibilities.

PE-02: PHYSICAL ACCESS AUTHORIZATIONS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides;
b. Issue authorization credentials for facility access;
c. Review the access list detailing authorized facility access by individuals at the frequency specified in Std.02; and
d. Remove individuals from the facility access list when access is no longer

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Develop and keep current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and issue appropriate authorization credentials. [Source: DIR Control Standards Catalog PE-2]

Std.02 — Access log review minimum frequency by system categorization:

a. Low — At least annually;
b. Moderate — At least quarterly;
c. High — Monthly.

Std.03 — Ensure authorization credential systems (for example, card/badge creation systems, card readers) are controlled and managed by authorized personnel.

Std.04 — Issue authorization credentials (for example, badges) providing only the level of access required to complete the individual's job responsibilities.

Std.05 — Revoke authorizations in accordance with PS-04, PS-05, and other applicable requirements.

SUPPLEMENTAL GUIDANCE

Physical access authorizations apply to employees and visitors. Individuals with permanent physical access authorization credentials are not considered visitors. Authorization credentials include ID badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Physical access authorizations may not be necessary to access certain areas within facilities that are designated as publicly accessible.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FIPS 201; NIST SP 800-73-4, 800-76-2, 800-78-4; FBI CJIS CSP v5.9	AT-3, AU-9, IA-4, MA-5, MP-2, PE-3, PE-4, PE-5, PE-8, PM-12, PS-3, PS-4, PS-5, PS-6.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Physical and environmental protection policy; procedures addressing physical access authorizations; authorized personnel access list; authorization credentials; physical access list reviews; physical access termination records and associated documentation; system security plan; other relevant documents or records.

Interview: Organizational personnel with physical access authorization responsibilities; organizational personnel with physical access to system facility; organizational personnel with information security responsibilities.

Test: Organizational processes for physical access authorizations; automated mechanisms supporting and/or implementing physical access authorizations.

PE-02(01): ACCESS BY POSITION / ROLE

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization authorizes physical access to the facility where the information system resides based on position or role.

AGENCY IMPLEMENTATION STANDARDS

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.01 — Develop and keep current a list of personnel with authorized access to the facility where the CJIS information system resides.

Std.02 — The agency shall securely store digital and physical media within physically secure locations or controlled areas. The agency shall restrict access to digital and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data shall be encrypted per Section 5.10.1.2 of the FBI CJIS CSP.

SUPPLEMENTAL GUIDANCE

Implementing role-based access controls for physical access provides a further level of granularity in governing who can access facilities, and even certain parts of facilities, that store and process CJI.

The authorization of physical access to the facility should include considerations of whether the person needs access to CJIS and whether such access is permitted under the FBI CJIS CSP.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FBI CJIS CSP v5.9	AC-2, AC-3, AC-6.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Physical and environmental protection policy; procedures addressing physical access authorizations; physical access control logs or records; list of positions/roles and corresponding physical access authorizations; system entry and exit points; system security plan; other relevant documents or records.

Interview: Organizational personnel with physical access authorization responsibilities; organizational personnel with physical access to system facility; organizational personnel with information security responsibilities.

Test: Organizational processes for physical access authorizations; automated mechanisms supporting and/or implementing physical access authorizations.

PE-02(03): RESTRICT UNESCORTED ACCESS

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization restricts unescorted access to the facility where the information system resides to personnel with formal access authorizations for all information contained within the system.

AGENCY IMPLEMENTATION STANDARDS

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.01 — Develop and keep current a list of personnel with authorized access to the facility where the CJIS information system resides and issue credentials to authorized personnel.

Std.02 — The agency shall control all physical access points (except for those areas within the facility officially designated as publicly accessible) and shall verify individual access authorizations before granting access.

Std.03 — The agency shall control physical access by authenticating visitors before authorizing escorted access to the physically secure location (except for those areas designated as publicly accessible). The agency shall escort visitors at all times and monitor visitor activity.

SUPPLEMENTAL GUIDANCE

Due to the highly sensitive nature of classified information stored within certain facilities, it is important that individuals lacking sufficient security clearances, access approvals, or need to know, be escorted by individuals with appropriate credentials to ensure that such information is not exposed or otherwise compromised.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FBI CJIS CSP v5.9	PS-2, PS-6.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Physical and environmental protection policy; procedures addressing physical access authorizations; authorized personnel access list; security clearances; access authorizations; access credentials; physical access control logs or records; system security plan; other relevant documents or records.

Interview: Organizational personnel with physical access authorization responsibilities; organizational personnel with physical access to the system facility; organizational personnel with information security responsibilities.

Test: Organizational processes for physical access authorizations; automated mechanisms supporting and/or implementing physical access authorizations.

PE-03: PHYSICAL ACCESS CONTROL

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Enforce physical access authorizations at entry and exit points as defined in Std.01 by:

1. Verifying individual access authorizations before granting access to the facility; and
2. Controlling ingress and egress to the facility using physical access devices (for example, keys, locks, combinations, card readers) and/or guards;

b. Maintain physical access audit logs for entry and exit points as defined in Std.01;

c. Control access to areas within the facility designated as publicly accessible by implementing the following controls: controls as defined in Std.02;

d. Escort visitors and control visitor activity in all areas of the facility not designated as publicly accessible;

e. Secure keys, combinations, and other physical access devices;

f. Inventory organization-owned physical access devices every 90 days; and

g. Change combinations and keys when first installed or before use if a default is provided by the vendor, annually, and whenever there is a theft or security violation in the area being protected, and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Control all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facility. [Source: DIR Control Standards Catalog PE-3]

Std.02 — Control access to areas officially designated as publicly accessible in accordance with the assessment of risk. Use identification and/or access badges in conjunction with access control readers (card readers), security guards, closed-circuit TV cameras and monitors, and sign-in/sign-out sheets to control entry to district and HQ facilities. Restrict access to grounds/facilities to authorized persons only.

Std.03 — Retain access records, entry and exit logs, and visitor logs in accordance with records retention or other state or federal requirements.

Std.04 — Control data center/facility access by use of door and window locks and, for moderate or high-baseline systems, security personnel or physical authentication devices, such as biometrics and/or smart card/PIN combination.

Std.05 — Store and operate servers in physically secure environments and, for moderate or high-baseline servers, grant access to explicitly authorized personnel only. Access is monitored and recorded.

Std.06 — Physically secure access to computer, paper, or other systems containing DFPS Sensitive, Confidential, or Controlled Information from unauthorized personnel and theft (for example, through the use of door locks, cable locks, storing laptops in the trunk of the car instead of the passenger area, etc.).

Std.07 — Record the date that keys and combinations are changed and the identity of the person making those changes in the system security plan. [Source: FedRAMP Continuous Monitoring Strategy & Guide]

SUPPLEMENTAL GUIDANCE

Physical access control applies to employees and visitors. Individuals with permanent physical access authorizations are not considered visitors. Physical access controls for publicly accessible areas may include physical access control logs/records, guards, or physical access devices and barriers to prevent movement from publicly accessible areas to non-public areas. Organizations determine the types of guards needed, including professional security staff, system users, or administrative staff. Physical access devices include keys, locks, combinations, biometric readers, and card readers. Physical access control systems comply with applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural, automated, or some combination thereof.

Physical access points can include facility access points, interior access points to systems that require supplemental access controls, or both. Components of systems may be in areas designated as publicly accessible with organizations controlling access to the components.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FIPS 201; NIST SP 800-73-4, 800-76-2, 800-78-4, 800-116; FBI CJIS CSP v5.9	AT-3, AU-2, AU-6, AU-9, AU-13, CP-10, IA-3, IA-8, MA-5, MP-2, MP-4, PE-2, PE-4, PE-5, PE-8, PS-2, PS-3, PS-6, PS-7, RA-3, SC-28, SI-4, SR-3.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; inventory records of physical access control devices; system entry and exit points; records of key and lock combination changes; storage locations for physical access control devices; physical access control devices; list of security safeguards controlling access to designated publicly accessible areas within facility; system security plan; other relevant documents or records.

Interview: Organizational personnel with physical access control responsibilities; organizational personnel with information security responsibilities.

Test: Organizational processes for physical access control; automated mechanisms supporting and/or implementing physical access control; physical access control devices.

PE-03(01): INFORMATION SYSTEM ACCESS

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility at all DFPS-managed facilities containing one or more components of the CJIS system.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Sections 5.9.1.1 – 5.9.1.8 of the FBI CJIS CSP describe the physical controls required in order to be considered a physically secure location, while Sections 5.2 and 5.12, respectively, describe the minimum security awareness training and personnel security controls required for unescorted access to a physically secure location. Sections 5.5, 5.6.2.2.1, and 5.10 describe the requirements for technical security controls required to access CJI from within the perimeter of a physically secure location without Advanced Authentication.

SUPPLEMENTAL GUIDANCE

Control of physical access to the system provides additional physical security for those areas within facilities where there is a concentration of system components.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FIPS 201; NIST SP 800-73-4, 800-76-2, 800-78-4, 800-116; FBI CJIS CSP v5.9	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; physical access control devices; access authorizations; access credentials; system entry and exit points; list of areas within the facility containing concentrations of system components or system components requiring additional physical protection; system security plan; other relevant documents or record.

Interview: Organizational personnel with physical access authorization responsibilities; organizational personnel with information security responsibilities.

Test: Organizational processes for physical access control to the information system/components; automated mechanisms supporting and/or implementing physical access control for facility areas containing system components.

PE-03(03): CONTINUOUS GUARDS / ALARMS / MONITORING

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization employs guards and/or alarms to monitor every physical access point to the facility where the information system resides 24 hours per day, 7 days per week.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

None.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FBI CJIS CSP v5.9	CP-6, CP-7, PE-6.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; physical access control devices; facility surveillance records; facility layout documentation; system entry and exit points; system security plan; other relevant documents or records.

Interview: Organizational personnel with physical access control responsibilities; organizational personnel with information security responsibilities.

Test: Organizational processes for physical access control to the facility where the system resides; automated mechanisms supporting and/or implementing physical access control for the facility where the system resides.

PE-04: ACCESS CONTROL FOR TRANSMISSION MEDIUM

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization controls physical access to network and information system distribution and transmission lines within organizational facilities using security safeguards defined in Stds.01-03.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — For systems whether on DFPS property or housed in infrastructure service provider's facilities, control physical access to moderate and high-impact systems' distribution and transmission lines by locking wire cabinets, disconnecting or locking spare jacks, and protecting cabling by conduit or cable trays.

Std.02 — Limit, monitor, and restrict physical access to moderate and high-impact systems and high-volume media storage areas through automated systems or guard stations.

Std.03 — Control physical access to sensitive areas for onsite personnel. Access must be authorized and based on individual job function in accordance with access control policy; revoked immediately upon termination; auditable; and processes must be in place to retrieve or disable physical access mechanisms such as keys and access cards at need.

SUPPLEMENTAL GUIDANCE

Security controls applied to system distribution and transmission lines prevent accidental damage, disruption, and physical tampering. Such controls may also be necessary to prevent eavesdropping or modification of unencrypted transmissions. Security controls used to control physical access to system distribution and transmission lines include disconnected or locked spare jacks, locked wiring closets, protection of cabling by conduit or cable trays, and wiretapping sensors.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog.	AT-3, IA-4, MP-2, MP-4, PE-2, PE-3, PE-5, PE-9, SC-7, SC-8.

Federal: FBI CJIS CSP v5.9	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Physical and environmental protection policy; procedures addressing access control for transmission mediums; system design documentation; facility communications and wiring diagrams; list of physical security safeguards applied to system distribution and transmission lines; system security plan; other relevant documents or records.

Interview: Organizational personnel with physical access control responsibilities; organizational personnel with information security responsibilities.

Test: Organizational processes for access control to distribution and transmission lines; automated mechanisms/security safeguards supporting and/or implementing access control to distribution and transmission lines.

PE-05: ACCESS CONTROL FOR OUTPUT DEVICES

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization controls physical access to output from devices defined in Std.01 to prevent unauthorized individuals from obtaining the output.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Secure physical access to paper, computers, or other systems containing DFPS Sensitive, Confidential, or Controlled Information from unauthorized personnel and from theft. This includes, but is not limited to, using door locks and cable locks, storing portable devices in locked containers during transportation, and refraining from displaying or leaving unsecured material in plain view or disable physical access mechanisms such as keys and access cards at need.

SUPPLEMENTAL GUIDANCE

Controlling physical access to output devices includes placing output devices in locked rooms or other secured areas with keypad or card reader access controls and allowing access to authorized individuals only, placing output devices in locations that can be monitored by personnel, installing monitor or screen filters, and using headphones.

Examples of output devices include monitors, printers, scanners, audio devices, facsimile machines, and copiers.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FBI CJIS CSP v5.9	PE-2, PE-3, PE-4, PE-18.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Physical and environmental protection policy; procedures addressing access control for display medium; facility layout of system components; actual displays from system components; list of output devices and associated outputs requiring physical access controls; physical access control logs or records for areas containing output devices and related outputs; system security plan; other relevant documents or records.

Interview: Organizational personnel with physical access control responsibilities; organizational personnel with information security responsibilities.

Test: Organizational processes for access control to output devices; automated mechanisms supporting and/or implementing access control to output devices.

PE-06: MONITORING PHYSICAL ACCESS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents;

b. Review physical access logs at the frequency specified in Std.02 and upon occurrence of events or potential indications of events as specified in the incident response policy and procedures; and

c. Coordinate results of reviews and investigations with the organizational incident response capability.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Monitor physical access to the information system to detect and respond to physical security incidents. [Source: DIR Control Standards Catalog PE-6]

Std.02 — Access log review minimum frequency by system categorization:

a. Low — At least annually;
b. Moderate — At least quarterly;
c. High — Monthly.

Std.03 — Investigate and respond to detected physical access activities in accordance with the incident response policy.

SUPPLEMENTAL GUIDANCE

Physical access monitoring includes publicly accessible areas within organizational facilities. Examples of physical access monitoring include the employment of guards, video surveillance equipment (i.e., cameras), and sensor devices. Reviewing physical access logs can help identify suspicious activity, anomalous events, or potential

threats. The reviews can be supported by audit logging controls, such as AU-02, if the access logs are part of an automated system. Organizational incident response capabilities include investigations of physical security incidents and responses to the incidents. Incidents include security violations or suspicious physical access activities. Suspicious physical access activities include accesses outside of normal work hours, repeated accesses to areas not normally accessed, accesses for unusual lengths of time, and out-of-sequence accesses.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FBI CJIS CSP v5.9	AU-2, AU-6, AU-9, AU-12, CA-7, CP-10, IR-4, IR-8.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Physical and environmental protection policy; procedures addressing physical access monitoring; physical access logs or records; physical access monitoring records; physical access log reviews; system security plan; other relevant documents or records.

Interview: Organizational personnel with physical access monitoring responsibilities; organizational personnel with incident response responsibilities; organizational personnel with information security responsibilities.

Test: Organizational processes for monitoring physical access; automated mechanisms supporting and/or implementing physical access monitoring; automated mechanisms supporting and/or implementing the review of physical access logs.

PE-06(01): INTRUSION ALARMS / SURVEILLANCE EQUIPMENT

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization monitors physical intrusion alarms and surveillance equipment.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Provide real-time physical intrusion alarms and surveillance equipment for facilities hosting DFPS systems.

SUPPLEMENTAL GUIDANCE

Physical intrusion alarms can be employed to alert security personnel when unauthorized access to the facility is attempted. Alarm systems work in conjunction with physical barriers, physical access control systems, and security guards by triggering a response when these other forms of security have been compromised or breached. Physical intrusion alarms can include different types of sensor devices, such as motion sensors, contact sensors, and broken glass sensors. Surveillance equipment includes video cameras installed at strategic locations throughout the facility.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FBI CJIS CSP v5.9	AU-2, AU-6, AU-9, AU-12, CA-7, CP-10, IR-4, IR-8.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Physical and environmental protection policy; procedures addressing physical access monitoring; physical access logs or records; physical access monitoring records; physical access log reviews; system security plan; other relevant documents or records.

Interview: Organizational personnel with physical access monitoring responsibilities; organizational personnel with incident response responsibilities; organizational personnel with information security responsibilities.

Test: Organizational processes for monitoring physical access; automated mechanisms supporting and/or implementing physical access monitoring; automated mechanisms supporting and/or implementing the review of physical access logs.

PE-08: VISITOR ACCESS RECORDS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Maintain visitor access records to the facility where the system resides for three years, as required by the Texas State Records Retention Schedule;

b. Review visitor access records at the frequency defined in Std.02; and

c. Report anomalies in visitor access records to personnel with facility security responsibilities.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Maintain visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible). [Source: DIR Control Standards Catalog PE-8]

Std.02 — Access log review minimum frequency by system categorization:

a. a. Low — At least annually;
b. b. Moderate — At least quarterly;
c. c. High — Monthly.

Std.03 — Investigate and respond to detected physical access activities in accordance with the incident response policy.

SUPPLEMENTAL GUIDANCE

Visitor access records include, for example, names and organizations of persons visiting, visitor signatures, forms of identification, dates of access, entry and departure times, purposes of visits, and names and organizations of persons visited. Visitor access records are not required for publicly accessible areas.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FBI CJIS CSP v5.9	PE-2, PE-3, PE-6.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Physical and environmental protection policy; procedures addressing visitor access records; visitor access control logs or records; visitor access record or log reviews; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records.

Interview: Organizational personnel with visitor access record responsibilities; organizational personnel with information security and privacy responsibilities.

Test: Organizational processes for maintaining and reviewing visitor access records; automated mechanisms supporting and/or implementing maintenance and review of visitor access records.

PE-09: POWER EQUIPMENT AND CABLING

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization protects power equipment and power cabling for the system from damage and destruction.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Organizations determine the types of protection necessary for the power equipment and cabling employed at different locations that are both internal and external to organizational facilities and environments of operation. Types of power equipment and cabling include internal cabling and uninterruptable power sources in offices or data centers, generators, and power cabling outside of buildings, and power sources for self-contained components such as satellites, vehicles, and other deployable systems.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog.	PE-4.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Physical and environmental protection policy; procedures addressing power equipment/cabling protection; facilities housing power equipment/cabling; system security plan; other relevant documents or records.

Interview: Organizational personnel with the responsibility to protect power equipment/cabling; organizational personnel with information security responsibilities.

Test: Automated mechanisms supporting and/or implementing protection of power equipment/cabling.

PE-10: EMERGENCY SHUTOFF

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization:

a. Provide the capability of shutting off power to systems or individual system components as identified in contingency plans in emergency situations;

b. Place emergency shutoff switches or devices in location by system or system component as defined in Std.01 to facilitate access for authorized personnel; and

c. Protect emergency power shutoff capability from unauthorized authorization.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Implement and maintain a master power switch or emergency cut-off switch, prominently marked, and protected against accidental activation by a cover, for data centers, servers, and mainframe rooms.

Std.02 — Document the location of emergency shutoff switches or devices in contingency plans.

Std.03 — Provide appropriate personnel with training on safe operation of emergency power shutoffs.

SUPPLEMENTAL GUIDANCE

Emergency power shutoff primarily applies to organizational facilities that contain concentrations of system resources, including data centers, mainframe computer rooms, server rooms, and areas with computer-controlled machinery.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog.	PE-15.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Physical and environmental protection policy; procedures addressing power source emergency shutoff; emergency shutoff controls or switches; locations housing emergency shutoff switches and devices; security safeguards protecting the emergency power shutoff capability from unauthorized activation; system security plan; other relevant documents or records.

Interview: Organizational personnel with the responsibility for the emergency power shutoff capability (both implementing and using the capability); organizational personnel with information security responsibilities.

Test: Automated mechanisms supporting and/or implementing emergency power shutoff.

PE-11: EMERGENCY POWER

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization provides an uninterruptible power supply to facilitate an orderly shutdown of the system or transition of the system to long-term alternate power in the event of a primary power source loss.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Transition plans for critical systems must be documented in the contingency plan. UPS for critical systems may be installed centrally or locally, and must be sized to permit transition to long-term alternate power.

Std.02 — For non-critical systems, UPS must be sized, at a minimum, so that the system can be shut down safely. [Source: NIST SP 800-82]

Std.03 — UPS must be tested at least annually and prior to seasons of expected events (for example, hurricane season).

SUPPLEMENTAL GUIDANCE

An uninterruptible power supply (UPS) is an electrical system or mechanism that provides emergency power when there is a failure of the main power source. A UPS is typically used to protect computers, data centers, telecommunication equipment, or other electrical equipment where an unexpected power disruption could cause injuries, fatalities, serious mission or business disruption, or loss of data or information. A UPS differs from an emergency power system or backup generator in that the UPS provides near-instantaneous protection from unanticipated power interruptions from the main power source by providing energy stored in batteries,

supercapacitors, or flywheels. The battery duration of a UPS is relatively short but provides sufficient time to start a standby power source, such as a backup generator, or properly shut down the system.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog.	AT-3, CP-2, CP-7.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Physical and environmental protection policy; procedures addressing emergency power; uninterruptible power supply; uninterruptible power supply documentation; uninterruptible power supply test records; system security plan; other relevant documents or records.

Interview: Organizational personnel with the responsibility for emergency power and/or planning; organizational personnel with information security responsibilities

Test: Automated mechanisms supporting and/or implementing uninterruptible power supply; the uninterruptable power supply.

PE-11(01): LONG-TERM ALTERNATE POWER SUPPLY - MINIMAL OPERATIONAL CAPABILITY

Priority: P1

Baseline(s): High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization provides an alternate power supply for the system that is activated manually or automatically and that can maintain minimally required operational capability in the event of an extended loss of the primary power source.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Test the equipment:

a. On a schedule that complies with manufacturer recommendations and local, state, and federal requirements;
b. As part of full-scale contingency testing;
c. After use during contingency events; and
d. At least once in every three-year period (if no test has been performed per requirements above)

Std.02 — Document the alternate power supply in the contingency plan for the system, including supporting systems for major applications.

SUPPLEMENTAL GUIDANCE

Provision of an alternate power supply with minimal operating capability can be satisfied by accessing a secondary commercial power supply or other external power supply.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog.	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Physical and environmental protection policy; procedures addressing emergency power; alternate power supply; alternate power supply documentation; alternate power supply test records; system security plan; other relevant documents or records.

Interview: Organizational personnel with the responsibility for emergency power and/or planning; organizational personnel with information security responsibilities.

Test: Automated mechanisms supporting and/or implementing alternate power supply; the alternate power supply.

PE-12: EMERGENCY LIGHTING

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization employs and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Employ and maintain automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes. [Source: DIR Control Standards Catalog PE-12]

SUPPLEMENTAL GUIDANCE

The provision of emergency lighting applies primarily to organizational facilities that contain concentrations of system resources, including data centers, server rooms, and mainframe computer rooms. Emergency lighting provisions for the system are described in the contingency plan for the organization. If emergency lighting for the system fails or cannot be provided, organizations consider alternate processing sites for power-related contingencies.

REFERENCES	RELATED CONTROLS

Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog.	CP-2, CP-7.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Physical and environmental protection policy; procedures addressing emergency lighting; emergency lighting documentation; emergency lighting test records; emergency exits and evacuation routes; areas/locations within facility supporting essential missions and business functions; system security plan; other relevant documents or records.

Interview: Organizational personnel with the responsibility for emergency lighting and/or planning; organizational personnel with information security responsibilities.

Test: Automated mechanisms supporting and/or implementing the emergency lighting capability.

PE-13: FIRE PROTECTION

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization employs and maintains fire detection and suppression systems that are supported by an independent energy source.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Information resources shall be protected from environmental hazards. Designated employees shall monitor equipment and shall be trained in environmental control procedures and in desired response in case of emergencies or equipment problems. [Source: DIR Control Standards Catalog PE-13]

SUPPLEMENTAL GUIDANCE

The provision of fire detection and suppression systems applies primarily to organizational facilities that contain concentrations of system resources, including data centers, server rooms, and mainframe computer rooms. Fire detection and suppression systems that may require an independent energy source include sprinkler systems and smoke detectors. An independent energy source is an energy source, such as a microgrid, that is separate, or can be separated, from the energy sources providing power for the other parts of the facility.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog.	AT-3.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Physical and environmental protection policy; procedures addressing fire protection; fire suppression and detection devices/systems; fire suppression and detection devices/systems documentation; test records of fire suppression and detection devices/systems; system security plan; other relevant documents or records.

Interview: Organizational personnel with the responsibility for emergency lighting and/or planning; organizational personnel with information security responsibilities.

Test: Automated mechanisms supporting and/or implementing fire suppression/detection devices/systems.

PE-13(01): DETECTION SYSTEMS — AUTOMATIC ACTIVATION AND NOTIFICATION

Priority: P1

Baseline(s): Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization employs fire detection systems that activate automatically and notify personnel as defined in the System Security Plan (SSP) and emergency responders as defined in the SSP or facility's safety plan in the event of a fire.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Ensure that fire detection systems are not tied into the facility's intrusion device system (IDS).

Std.02 — In accordance with local regulations, ensure facilities undergo fire marshal inspections and promptly resolve identified deficiencies.

SUPPLEMENTAL GUIDANCE

Organizations can identify personnel, roles, and emergency responders if individuals on the notification list need to have access authorizations or clearances (e.g., to enter to facilities where access is restricted due to the classification or impact level of information within the facility). Notification mechanisms may require independent energy sources to ensure that the notification capability is not adversely affected by the fire.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog.	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Physical and environmental protection policy; procedures addressing fire protection; facility housing the information system; alarm service-level agreements; test records of fire suppression and detection devices/systems; fire suppression and detection devices/systems documentation; alerts/notifications of fire events; system security plan; other relevant documents or records.

Interview: Organizational personnel with responsibilities for fire detection and suppression devices/systems; organizational personnel with responsibilities for notifying appropriate personnel, roles, and emergency responders of fires; organizational personnel with information security responsibilities.

Test: Automated mechanisms supporting and/or implementing fire detection devices/systems; activation of fire detection devices/systems (simulated); automated notifications.

PE-13(02): SUPPRESSION SYSTEMS — AUTOMATIC ACTIVATION AND NOTIFICATION

Priority: P1

Baseline(s): Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization:

a. Employ fire suppression systems that activate automatically and notify personnel as defined in the System Security Plan (SSP) and emergency responders as defined in the SSP or facility's safety plan; and

b. Employ an automatic fire suppression capability when the facility is not staffed on a continuous basis.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — In accordance with local regulations, ensure the facility undergoes fire marshal inspections and promptly resolve identified deficiencies.

Std.02 — Ensure that contingency plans account for suppression system impacts.

SUPPLEMENTAL GUIDANCE

Organizations can identify specific personnel, roles, and emergency responders if individuals on the notification list need to have appropriate access authorizations and/or clearances (e.g., to enter to facilities where access is restricted due to the impact level or classification of information within the facility). Notification mechanisms may require independent energy sources to ensure that the notification capability is not adversely affected by the fire.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog.	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Physical and environmental protection policy; procedures addressing fire protection; fire suppression and detection devices/systems documentation; facility housing the system; alarm service-level agreements; test records of fire suppression and detection devices/systems; system security plan; other relevant documents or records.

Interview: Organizational personnel with responsibilities for fire detection and suppression devices/systems; organizational personnel with responsibilities for providing automatic notifications of any activation of fire suppression devices/systems to appropriate personnel, roles, and emergency responders; organizational personnel with information security responsibilities.

Test: Automated mechanisms supporting and/or implementing fire suppression devices/systems; activation of fire suppression devices/systems (simulated); automated notifications.

PE-14: TEMPERATURE AND HUMIDITY CONTROLS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization:

a. Maintain temperature and humidity levels within the facility where the system resides at acceptable levels as specified in the documentation for the equipment being protected; and

b. Monitor environmental control levels at an acceptable frequency as specified in the documentation for the equipment being protected.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Regularly maintain, within acceptable levels, and monitor the temperature and humidity within the facility where the information system resides. [Source: DIR Control Standards Catalog PE-14]

Std.02 — Monitoring systems should be configured to generate an alert when environmental specifications such as temperature and humidity are exceeded. [Source: NIST SP 800-82]

SUPPLEMENTAL GUIDANCE

The provision of environmental controls applies primarily to organizational facilities that contain concentrations of system resources (e.g., data centers, mainframe computer rooms, and server rooms). Insufficient environmental controls, especially in very harsh environments, can have a significant adverse impact on the availability of systems and system components that are needed to support organizational mission and business functions.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog.	AT-3, CP-2.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Physical and environmental protection policy; procedures addressing temperature and humidity control; temperature and humidity controls; facility housing the system; temperature and humidity controls documentation; temperature and humidity records; system security plan; other relevant documents or records.

Interview: Organizational personnel with responsibilities for system environmental controls; organizational personnel with information security responsibilities.

Test: Automated mechanisms supporting and/or implementing the maintenance and monitoring of temperature and humidity levels.

PE-15: WATER DAMAGE PROTECTION

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization protects the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Protect the information system from water damage resulting from broken plumbing lines or other sources of water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel. [Source: DIR Control Standards Catalog PE-15]

SUPPLEMENTAL GUIDANCE

The provision of water damage protection primarily applies to organizational facilities that contain concentrations of system resources, including data centers, server rooms, and mainframe computer rooms. Isolation valves can be employed in addition to or in lieu of master shutoff valves to shut off water supplies in specific areas of concern without affecting entire organizations.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog.	AT-3, PE-10.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Physical and environmental protection policy; procedures addressing water damage protection; facility housing the system; master shutoff valves; list of key personnel with knowledge of location and activation procedures for master shutoff valves for the plumbing system; master shutoff valve documentation; system security plan; other relevant documents or records.

Interview: Organizational personnel with responsibilities for system environmental controls; organizational personnel with information security responsibilities,

Test: Master water-shutoff valves; organizational process for activating master water shutoff.

PE-15(01): AUTOMATION SUPPORT

Priority: P1

Baseline(s): High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization can detect the presence of water near the system and alert personnel or roles as identified in the System Security Plan (SSP) using automated mechanisms as identified in applicable SSPs.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Automated mechanisms include notification systems, water detection sensors, and alarms.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog.	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Physical and environmental protection policy; procedures addressing water damage protection; facility housing the system; automated mechanisms for water shutoff valves; automated mechanisms for detecting the presence of water in the vicinity of the system; alerts/notifications of water detection in system facility; system security plan; other relevant documents or records.

Interview: Organizational personnel with responsibilities for system environmental controls; organizational personnel with information security responsibilities.

Test: Automated mechanisms supporting and/or implementing water detection capabilities and alerts for the system.

PE-16: DELIVERY AND REMOVAL

Priority: P1	
Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Authorize and control system components and related items entering and exiting the facility; and

b. Maintain records of the system components.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Authorize, monitor, and control system components entering and exiting data processing facilities and maintain records of those items. [Source: DIR Control Standards Catalog PE-16]

SUPPLEMENTAL GUIDANCE

Automated mechanisms include notification systems, water detection sensors, and alarms.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** FBI CJIS CSP v5.9	CM-3, CM-8, MA-2, MA-3, MP-5, PE-20, SR-2, SR-3, SR-4, SR-6.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Physical and environmental protection policy; procedures addressing the delivery and removal of system components from the facility; facility housing the system; records of items entering and exiting the facility; system security plan; other relevant documents or records.

Interview: Organizational personnel with responsibilities for controlling system components entering and exiting the facility; organizational personnel with information security responsibilities.

Test: Organizational process for authorizing, monitoring, and controlling system-related items entering and exiting the facility; automated mechanisms supporting and/or implementing, authorizing, monitoring, and controlling system-related items entering and exiting the facility.

PE-17: ALTERNATE WORK SITE

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization:

a. Determine and document the alternate work sites in contingency plans allowed for use by employees;

b. Employ the following controls at alternate work sites: security and privacy controls equivalent to those applicable at the primary work site;

c. Assess the effectiveness of controls at alternate work sites; and

d. Provide a means for employees to communicate with information security and privacy personnel in case of incidents.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Alternate work sites (remote locations) must be identified in System Security Plans (SSPs) or contingency plans and available for business resumption activities in case of a disaster.

Std.02 — All equipment stored at alternate work sites must be secured when not in use and must be protected from damage and unauthorized access at all times.

SUPPLEMENTAL GUIDANCE

A "remote location" is a location outside the designated work location including, but not limited to, the employee's home, a satellite office, or another location from which an employee can safely perform work functions.

Alternate work sites include government facilities or the private residences of employees. While distinct from alternative processing sites, alternate work sites can provide readily available alternate locations during contingency operations. Organizations can define different sets of controls for specific alternate work sites or types of sites depending on the work-related activities conducted at the sites. Implementing and assessing the effectiveness of organization-defined controls and providing a means to communicate incidents at alternate work sites supports the contingency planning activities of organizations.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** NIST SP 800-46.	AC-17, AC-18, CP-7.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Physical and environmental protection policy; procedures addressing alternate work sites for organizational personnel; list of security controls required for alternate work sites; assessments of security controls at alternate work sites; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel approving the use of alternate work sites; organizational personnel using alternate work sites; organizational personnel assessing controls at alternate work sites; organizational personnel with information security and privacy responsibilities.

Test: Organizational processes for security and privacy at alternate work sites; automated mechanisms supporting alternate work sites; security and privacy controls employed at alternate work sites; means of communication between personnel at alternate work sites and security and privacy personnel.

PE-18: LOCATION OF INFORMATION SYSTEM COMPONENTS

Priority: P1

Baseline(s): High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization positions system components within the facility to minimize potential damage from physical and environmental hazards as identified in the facility risk assessment (to include water, HAZMAT, exhaust hoods and fans, and fuel storage areas) and to minimize the opportunity for unauthorized access

AGENCY IMPLEMENTATION STANDARDS

Std.01 — The organization considers the risks associated with physical and environmental hazards when planning new control system facilities or reviewing existing facilities. Risk mitigation strategies are documented in the control system security plan. [Source: Catalog of Control Systems Security: Recommendations for Standards Developers]

Std.02 — Document the physical location of system components in accordance with CM-08.

SUPPLEMENTAL GUIDANCE

Physical and environmental hazards include floods, fires, tornadoes, earthquakes, hurricanes, terrorism, vandalism, an electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation. Organizations consider the location of entry points where unauthorized individuals, while not being granted access, might nonetheless be near systems. Such proximity can increase the risk of unauthorized access to organizational communications using wireless packet sniffers or microphones, or unauthorized disclosure of information.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** FBI CJIS CSP v5.9.	CP-2, PE-5, PE-19, PE-20, RA-3.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Physical and environmental protection policy; procedures addressing the positioning of system components; documentation providing the location and position of system components within the facility; locations housing system components within the facility; list of physical and environmental hazards with the potential to damage system components within the facility; system security plan; other relevant documents or records.

Interview: Organizational personnel with responsibilities for positioning system components; organizational personnel with information security responsibilities.

Test: Organizational processes for positioning system components.

PE-18(01): FACILITY SITE

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

This control is withdrawn and incorporated into PE-23 but still referenced in the FBI CJIS Security Policy v5.9. Please see PE-23.

PE-20: ASSET MONITORING AND TRACKING

Priority: P1

Baseline(s): N/A	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization:

a. Employs organization-defined asset location technologies to track and monitor the location and movement of organization-defined assets that store CJIS information within organizational-defined control areas; and

b. Ensures that asset location technologies are employed in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — The organization employs remote device location (GPS) tracking (if two other required advanced authentication compensating controls are not in place) to track and monitor the location and movement of agency-issued smartphones and tablets that process CJI. Device tracking is not currently required in the CJIS Security Policy but should be applied to agency owned devices where possible as a risk mitigation factor. Access to device tracking software or applications within the organization should be controlled with limits and formal processes required to initiate a tracking action. [Source: FBI CJIS CSP v5.9]

SUPPLEMENTAL GUIDANCE

Physical and environmental hazards include floods, fires, tornadoes, earthquakes, hurricanes, terrorism, vandalism, an electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation. Organizations consider the location of entry points where unauthorized individuals, while not being granted access, might nonetheless be near systems. Such proximity can increase the risk of unauthorized access to organizational communications using wireless packet sniffers or microphones, or unauthorized disclosure of information.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** FBI CJIS CSP v5.9.	CM-8, PE-16, PM-8.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Physical and environmental protection policy; procedures addressing asset monitoring and tracking; documentation showing the use of asset location technologies; system configuration documentation; list of organizational assets requiring tracking and monitoring; asset monitoring and tracking records; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with asset monitoring and tracking responsibilities; legal counsel; organizational personnel with information security and privacy responsibilities.

Test: Organizational processes for tracking and monitoring assets; automated mechanisms supporting and/or implementing the tracking and monitoring of assets.

PE-23: FACILITY LOCATION

Priority: P1

Baseline(s): N/A	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization:

a. Plan the location or site of the facility where the system resides considering physical and environmental hazards; and

b. For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — The organization considers the risks associated with physical and environmental hazards when planning new control system facilities or reviewing existing facilities. Risk mitigation strategies are documented in the control system security plan. [Source: Catalog of Control Systems Security: Recommendations for Standards Developers]

Std.02 — Document the physical location of system components in accordance with CM-08.

SUPPLEMENTAL GUIDANCE

Physical and environmental hazards include floods, fires, tornadoes, earthquakes, hurricanes, terrorism, vandalism, an electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation. The location of system components within the facility is addressed in PE-18.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal:** FBI CJIS CSP v5.9.	CP-2, PE-18, PE-19, PM-8, PM-9, RA-3.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Physical and environmental protection policy; physical site planning documents; organizational assessment of risk; contingency plan; risk mitigation strategy documentation; system security plan; other relevant documents or records.

Interview: Organizational personnel with site selection responsibilities for the facility housing the system; organizational personnel with risk mitigation responsibilities; organizational personnel with information security responsibilities.

Test: Organizational processes for site planning.

(PL) PLANNING

DFPS requires the development, documentation, periodic update, and implementation of security plans for information systems within the DFPS environment. DFPS also requires that those security plans describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

The intended audience for this Control includes, but is not limited to, information resource owners and custodians. Information resource owner, or designee, is responsible for ensuring that the planning measures described in this Control are implemented with the assistance of the DFPS Office of Information Security.

PL-01: SECURITY PLANNING POLICY AND PROCEDURES

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Develop, document, and disseminate to appropriate personnel:

1. Organization-level planning policy that:
   a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;

b. Designate a senior management official as defined in the planning policy to manage the development, documentation, and dissemination of the planning policy and procedures; and

c. Review and update the current physical and environmental protection:

1. Policy every two (2) years and following major changes to legislation or security requirements; and
2. Procedures every two (2) years and following major changes to legislation or security requirements.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — As required by 1 TAC 202.23(a), DFPS delivers, at least annually, to the DFPS Commissioner a report on the DFPS information security program. [Source: DIR Control Standards Catalog PL-1]

Std.02 — The DFPS Commissioner or his/her designated representative(s) shall ensure that senior agency officials and information-owners, in collaboration with the Information Resources Manager/Chief Information Officer and Chief Information Security Officer, support the provision of information security for the information systems that support the operations and assets under their direct or indirect (e.g., cloud computing or outsourced) control. [Source: 1 TAC 202.20(3)]

Std.03 — The DFPS Chief Information Security Officer shall be responsible for:

a. Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks;

b. Providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities under 1 TAC 202; and

c. Developing and recommending policies and establishing procedures and practices, in cooperation with the agency Information Resources Manager, information-owners and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, or disclosure. [Source: 1 TAC 202.21(b)(3, 5, 8)]

SUPPLEMENTAL GUIDANCE

Planning policy and procedures for the controls in the PL family implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on their development. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission level or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission/business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to planning policy and procedures include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** 1 TAC 202.20(3); DIR Security Control Standards Catalog. **Federal**: OMB A-130; NIST SP 800-12, 800-18, 800-30, 800-39, 800-100; FBI CJIS CSP v5.9	PM-9, PS-8, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Planning policy and procedures; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with planning responsibilities; organizational personnel with information security and privacy responsibilities.

PL-02: SYSTEM SECURITY PLAN

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Develop security and privacy plans for the system that:
   1. Are consistent with the organization's enterprise architecture;
   2. Explicitly define the constituent system components;
   3. Describe the operational context of the system in terms of mission and business processes;
   4. Identify the individuals that fulfill system roles and responsibilities;
   5. Identify the information types processed, stored, and transmitted by the system;
   6. Provide the security categorization of the system, including supporting rationale;
   7. Describe any specific threats to the system that are of concern to the organization;
   8. Provide the results of a privacy risk assessment for systems processing personally identifiable information;
   9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;
   10. Provide an overview of the security and privacy requirements for the system;
   11. Identify any relevant control baselines or overlays, if applicable;
   12. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;
   13. Include risk determinations for security and privacy architecture and design decisions;
   14. Include security- and privacy-related activities affecting the system that require planning and coordination with individuals or groups as identified in organization plans (including system security plans (SSPs), contingency plans, and incident response plans); and
   15. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.
   16. Distribute copies of the plans and communicate subsequent changes to the plans to personnel or roles as identified in the SSP;
   17. Review the plans at least annually or when required due to system modifications or changes to the environment of operation (including new legislative requirements and newly discovered vulnerabilities);
   18. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and
   19. Protect the plans from unauthorized disclosure and modification

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Develop and implement a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan. [Source: DIR Control Standards Catalog PL-2]

Std.02 — Develop a System Security Plan (SSP) template consistent with the DFPS Information Security Minimum Baseline Standard.

Std.03 — Require that systems complete the SSP as part of the authorization process; and update to the approved SSP template prior to system authorization or re-authorization.

SUPPLEMENTAL GUIDANCE

Security plans relate security requirements to a set of security controls and control enhancements. Security plans also describe, at a high level, how the security controls and control enhancements meet those security requirements, but do not provide detailed, technical descriptions of the specific design or implementation of the controls/enhancements. Security plans contain sufficient information (including the specification of parameter values for assignment and selection statements either explicitly or by reference) to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk to organizational operations and assets, individuals, other organizations, and the Nation if the plan is implemented as intended. Organizations can also apply tailoring guidance to the security control baselines in Appendix D and CNSS Instruction 1253 to develop overlays for community-wide use or to address specialized requirements, technologies, or missions/environments of operation (e.g., DoD-tactical, Federal Public Key Infrastructure, or Federal Identity, Credential, and Access Management, space operations). Appendix I provides guidance on developing overlays.

Security plans need not be single documents; the plans can be a collection of various documents including documents that already exist. Effective security plans make extensive use of references to policies, procedures, and additional documents (e.g., design and implementation specifications) where more detailed information can be obtained. This reduces the documentation requirements associated with security programs and maintains security-related information in other established management/operational areas related to enterprise architecture, system development life cycle, systems engineering, and acquisition. For example, security plans do not contain detailed contingency plan or incident response plan information but instead provide explicitly or by reference, sufficient information to define what needs to be accomplished by those plans.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Information Security Minimum Baseline Standard. **State:** 1 TAC 202.20(3); DIR Security Control Standards Catalog. **Federal**: OMB A-130; NIST SP 800-18, 800-37, 800-160-1, 800-160-2; FBI CJIS CSP v5.9	AC-2, AC-6, AC-14, AC-17, AC-20, CA-2, CA-3, CA-7, CM-9, CM-13, CP-2, CP-4, IR-4, IR-8, MA-4, MA-5, MP-4, MP-5, PL-7, PL-8, PL-10, PL-11, PM-1, PM-7, PM-8, PM-9, PM-10, PM-11, RA-3, RA-8, RA-9, SA-5, SA-17, SA-22, SI-12, SR-2, SR-4.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Security and privacy planning policy; procedures addressing system security and privacy plan development and implementation; procedures addressing security and privacy plan reviews and updates; enterprise architecture documentation; system security plan; privacy plan; records of system security and privacy plan reviews and updates; security and privacy architecture and design documentation; risk assessments; risk assessment results; control assessment documentation; other relevant documents or records.

Interview: Organizational personnel with system security and privacy planning and plan implementation responsibilities; system developers; organizational personnel with information security and privacy responsibilities.

Test: Organizational processes for system security and privacy plan development, review, update, and approval; automated mechanisms supporting the system security and privacy plan.

PL-02(03): PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

This control is withdrawn and incorporated into PL-02 but still referenced in the FBI CJIS Security Policy v5.9. Please see PL-02.

PL-04: RULES OF BEHAVIOR

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;

b. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system;

c. Review and update the rules of behavior annually; and

d. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge annually.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS must define scope, behavior, and practices; compliance monitoring pertaining to users of information resources. [Source: DIR Control Standards Catalog PL-4]

Std.02 — The user of an information resource has the responsibility to:

a. Use the resource only for the purpose specified by the agency or information-owner;

b. Comply with information security controls and agency policies to prevent unauthorized or accidental disclosure, modification, or destruction; and

b. Formally acknowledge that they will comply with the security policies and procedures in a method determined by the DFPS Commisioner or his or her designated representative. [Source: 1 TAC 202.22(3)]

Std.03 — DFPS must enforce security policies and procedures for information resources designated for use by the public without requiring user participation or intervention. DFPS must require the acceptance of a banner or notice prior to use. [Source: 1 TAC 202.22(4)]

Std.04 — DFPS must develop a data use agreement for use by the agency that meets the particular needs of the agency and is consistent with rules adopted by the Texas Department of Information Resources that relate to information security standards for state agencies. [Source: TX Govt. Code 2054.135(a)]

Std.05 — DFPS must update the data use agreement at least biennially but may update the agreement at any time as necessary to accommodate best practices in data management. [Source: TX Govt. Code 2054.135(b)]

Std.06 — DFPS must distribute the data use agreement and each update to that agreement, to employees of the agency who handle sensitive information, including financial, medical, personnel, or student data. The employee shall sign the data use agreement distributed and each update to the agreement. [Source: TX Govt. Code 2054.135(c)]

Std.07 — To the extent possible, DFPS must provide employees described in TX Govt. Code 2054.135(c) with cybersecurity awareness training to coincide with the distribution of:

a. The data use agreement required under TX Govt. Code 2054.135(b); and
b. Each biennial update to that agreement. [Source: TX Govt. Code 2054.135(d)]

Std.08 — Users of an information resource must meet the standards established under "Confidential and Sensitive Information" within the DFPS Acceptable Use Agreement.

Std.09 — Users of an information resource must meet the standards established under Chapter 4: Employee Conduct of the DFPS Human Resources Manual.

SUPPLEMENTAL GUIDANCE

Rules of behavior represent a type of access agreement for organizational users. Other types of access agreements include nondisclosure agreements, conflict-of-interest agreements, and acceptable use agreements (see PS-06). Organizations consider rules of behavior based on individual user roles and responsibilities and differentiate between rules that apply to privileged users and rules that apply to general users. Establishing rules of behavior for some types of non-organizational users, including individuals who receive information from federal systems, is often not feasible given the large number of such users and the limited nature of their interactions with the systems. Rules of behavior for organizational and non-organizational users can also be established in AC-08. The related controls section provides a list of controls that are relevant to organizational rules of behavior. PL-04b, the documented acknowledgment portion of the control, may be satisfied by the literacy training and awareness and role-based training programs conducted by organizations if such training includes rules of behavior. Documented acknowledgements for rules of behavior include electronic or physical signatures and electronic agreement check boxes or radio buttons.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Acceptable Use Agreement; DFPS Human Resources Manual. **State:** 1 TAC 202.22(3), 1 TAC 202.22(4); TX Govt. Code 2054.135(a, b, c, d); DIR Security Control Standards Catalog. **Federal**: OMB A-130; NIST SP 800-18; FBI CJIS CSP v5.9	AC-2, AC-6, AC-8, AC-9, AC-17, AC-18, AC-19, AC-20, AT-2, AT-3, CM-11, IA-2, IA-4, IA-5, MP-7, PS-6, PS-8, SA-5, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Security and privacy planning policy; procedures addressing rules of behavior for system users; rules of behavior; signed acknowledgements; records for rules of behavior reviews and updates; other relevant documents or records.

Interview: Organizational personnel with responsibility for establishing, reviewing, and updating rules of behavior; organizational personnel with responsibility for literacy training and awareness and role-based training; organizational personnel who are authorized users of the system and have signed and resigned rules of behavior; organizational personnel with information security and privacy responsibilities.

Test: Organizational processes for establishing, reviewing, disseminating, and updating rules of behavior; automated mechanisms supporting and/or implementing the establishment, review, dissemination, and update of rules of behavior.

PL-04(01): SOCIAL MEDIA AND NETWORKING RESTRICTIONS

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Users of an information resource must meet the standards established under Chapter 4: Employee Conduct, subsection C: Social Media within the DFPS Human Resources Manual.

SUPPLEMENTAL GUIDANCE

Social media, social networking, and external site/application usage restrictions address rules of behavior related to the use of social media, social networking, and external sites when organizational personnel are using such sites for official duties or in the conduct of official business, when organizational information is involved in social media and social networking transactions, and when personnel access social media and networking sites from organizational systems. Organizations also address specific rules that prevent unauthorized entities from obtaining non-public organizational information from social media and networking sites either directly or through inference. Non-public information includes personally identifiable information and system account information.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Human Resources Manual. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; NIST SP 800-18; FBI CJIS CSP v5.9	AC-22, AU-13.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Security and privacy planning policy; procedures addressing rules of behavior for system users; rules of behavior; training policy; other relevant documents or records.

Interview: Organizational personnel with responsibility for establishing, reviewing, and updating rules of behavior; organizational personnel with responsibility for literacy training and awareness and role-based training; organizational personnel who are authorized users of the system and have signed rules of behavior; organizational personnel with information security and privacy responsibilities.

Test: Organizational processes for establishing rules of behavior; automated mechanisms supporting and/or implementing the establishment of rules of behavior.

PL-07: SECURITY CONCEPT OF OPERATIONS

Baseline(s): N/A	Overlay(s): CJIS

CONTROL REQUIREMENTS

For systems processing CJIS data, the following additional Implementation Standard applies:

The organization:

a. Develop a Concept of Operations (CONOPS) for the system describing how the organization intends to operate the system from the perspective of information security and privacy; and

b. Review and update the CONOPS biannually.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

The security CONOPS may be included in the security plan for the information system or in other system development life cycle-related documents, as appropriate. Changes to the CONOPS are reflected in ongoing updates to the security plan, the information security architecture, and other appropriate organizational documents (e.g., security specifications for procurements/acquisitions, system development life cycle documents, and systems/security engineering documents).

REFERENCES	RELATED CONTROLS
Federal: FBI CJIS CSP v5.9	PL-2, SA-2, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Security and privacy planning policy; procedures addressing rules of behavior for system users; rules of behavior; training policy; other relevant documents or records.

Interview: Organizational personnel with responsibility for establishing, reviewing, and updating rules of behavior; organizational personnel with responsibility for literacy training and awareness and role-based training; organizational personnel who are authorized users of the system and have signed rules of behavior; organizational personnel with information security and privacy responsibilities.

Test: Organizational processes for establishing rules of behavior; automated mechanisms supporting and/or implementing the establishment of rules of behavior.

PL-08: INFORMATION SECURITY ARCHITECTURE

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Develop security and privacy architectures for the system that:

   1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;
   2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals;
   3. Describe how the architectures are integrated into and support the enterprise architecture; and
   4. Describe any assumptions about, and dependencies on, external systems and services;

b. Review and update the architectures annually or when changes to the information system or its environment warrant to reflect changes in the enterprise architecture; and

c. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

This control addresses actions taken by organizations in the design and development of information systems. The information security architecture at the individual information system level is consistent with and complements the more global, organization-wide information security architecture described in PM-7 that is integral to and developed as part of the enterprise architecture. The information security architecture includes an architectural description, the placement/allocation of security functionality (including security controls), security-related information for external interfaces, information being exchanged across the interfaces, and the protection mechanisms associated with each interface. In addition, the security architecture can include other important security-related information, for example, user roles and access privileges assigned to each role, unique security requirements, the types of information processed, stored, and transmitted by the information system, restoration priorities of information and information system services, and any other specific protection needs.

In today's modern architecture, it is becoming less common for organizations to control all information resources. There are going to be key dependencies on external information services and service providers. Describing such dependencies in the information security architecture is important to developing a comprehensive mission/business protection strategy. Establishing, developing, documenting, and maintaining under configuration control, a baseline configuration for organizational information systems is critical to implementing and maintaining an effective information security architecture. The development of the information security architecture is coordinated with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO)

to ensure that security controls needed to support privacy requirements are identified and effectively implemented. PL-8 is primarily directed at organizations (i.e., internally focused) to help ensure that organizations develop an information security architecture for the information system, and that the security architecture is integrated with or tightly coupled to the enterprise architecture through the organization-wide information security architecture. In contrast, SA-17 is primarily directed at external information technology product/system developers and integrators (although SA-17 could be used internally within organizations for in-house system development). SA-17, which is complementary to PL-8, is selected when organizations outsource the development of information systems or information system components to external entities, and there is a need to demonstrate/show consistency with the organization's enterprise architecture and information security architecture.

SP 800-160-1 provides guidance on the use of security architectures as part of the system development life cycle process. OMB M-19-03 requires the use of the systems security engineering concepts described in SP 800-160-1 for high value assets. Security and privacy architectures are reviewed and updated throughout the system development life cycle, from analysis of alternatives through review of the proposed architecture in the RFP responses to the design reviews before and during implementation (e.g., during preliminary design reviews and critical design reviews).

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; NIST SP 800-160-1, 800-160-2FBI CJIS CSP v5.9	CM-2, CM-6, PL-2, PL-7, PL-9, PM-5, PM-7, RA-9, SA-3, SA-5, SA-8, SA-17, SC-7.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Security and privacy planning policy; procedures addressing information security and privacy architecture development; procedures addressing information security and privacy architecture reviews and updates; enterprise architecture documentation; information security and privacy architecture documentation; system security plan; privacy plan; security and privacy CONOPS for the system; records of information security and privacy architecture reviews and updates; other relevant documents or records.

Interview: Organizational personnel with security and privacy planning and plan implementation responsibilities; organizational personnel with information security and privacy architecture development responsibilities; organizational personnel with information security and privacy responsibilities.

Test: Organizational processes for developing, reviewing, and updating the information security and privacy architecture; automated mechanisms supporting and/or implementing the development, review, and update of the information security and privacy architecture.

PL-09: CENTRAL MANAGEMENT

Baseline(s): N/A	Overlay(s): CJIS

CONTROL REQUIREMENTS

Centrally manage organization-wide privacy common controls as designated by the agency and related processes.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Document organization-wide privacy common controls in Information Security Program Plan.

SUPPLEMENTAL GUIDANCE

Central management refers to organization-wide management and implementation of selected controls and processes. This includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed controls and processes. As the central management of controls is generally associated with the concept of common (inherited) controls, such management promotes and facilitates standardization of control implementations and management and the judicious use of organizational resources. Centrally managed controls and processes may also meet independence requirements for assessments in support of initial and ongoing authorizations to operate and as part of organizational continuous monitoring.

Automated tools (e.g., security information and event management tools or enterprise security monitoring and management tools) can improve the accuracy, consistency, and availability of information associated with centrally managed controls and processes. Automation can also provide data aggregation and data correlation capabilities; alerting mechanisms; and dashboards to support risk-based decision-making within the organization.

As part of the control selection processes, organizations determine the controls that may be suitable for central management based on resources and capabilities. It is not always possible to centrally manage every aspect of a control. In such cases, the control can be treated as a hybrid control with the control managed and implemented centrally or at the system level. The controls and control enhancements that are candidates for full or partial central management include but are not limited to: AC-2(1), AC-2(2), AC-2(3), AC-2(4), AC-4(all), AC-17(1), AC-17(2), AC-17(3), AC-17(9), AC-18(1), AC-18(3), AC-18(4), AC-18(5), AC-19(4), AC-22, AC-23, AT-2(1), AT-2(2), AT-3(1), AT-3(2), AT-3(3), AT-4, AU-3, AU-6(1), AU-6(3), AU-6(5), AU-6(6), AU-6(9), AU-7(1), AU-7(2), AU-11, AU-13, AU-16, CA-2(1), CA-2(2), CA-2(3), CA-3(1), CA-3(2), CA-3(3), CA-7(1), CA-9, CM-2(2), CM-3(1), CM-3(4), CM-4, CM-6, CM-6(1), CM-7(2), CM-7(4), CM-7(5), CM-8(all), CM-9(1), CM-10, CM-11, CP-7(all), CP-8(all), SC-43, SI-2, SI-3, SI-4(all), SI-7, SI-8.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; NIST SP 800-37; FBI CJIS CSP v5.9	PL-8, PM-9.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Security and privacy planning policy; procedures addressing security and privacy plan development and implementation; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with security and privacy planning and plan implementation responsibilities; organizational personnel with responsibilities for planning/implementing central management of controls and related processes; organizational personnel with information security and privacy responsibilities.

Test: Organizational processes for the central management of controls and related processes; automated mechanisms supporting and/or implementing central management of controls and related processes.

PL-10: BASELINE SELECTION

Baseline(s): N/A	Overlay(s): CJIS

CONTROL REQUIREMENTS

Select a control baseline for the system.

AGENCY IMPLEMENTATION STANDARDS

Std.01 —Systems must be categorized and information classified in accordance with DFPS Data Classification Policy and a control baseline assigned that aligns with or exceeds the baselines in the DFPS Information Security Minimum Baseline Standard.

SUPPLEMENTAL GUIDANCE

Control baselines are predefined sets of controls specifically assembled to address the protection needs of a group, organization, or community of interest. Controls are chosen for baselines to either satisfy mandates imposed by laws, executive orders, directives, regulations, policies, standards, and guidelines or address threats common to all users of the baseline under the assumptions specific to the baseline. Baselines represent a starting point for the protection of individuals' privacy, information, and information systems with subsequent tailoring actions to manage risk in accordance with mission, business, or other constraints (see PL-11). Federal control baselines are provided in SP 800-53B. The selection of a control baseline is determined by the needs of stakeholders. Stakeholder needs consider mission and business requirements as well as mandates imposed by applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. For example, the control baselines in SP 800-53B are based on the requirements from FISMA and PRIVACT. The requirements, along with the NIST standards and guidelines implementing the legislation, direct organizations to select one of the control baselines after the reviewing the information types and the information that is processed, stored, and transmitted on the system; analyzing the potential adverse impact of the loss or compromise of the information or system on the organization's operations and assets, individuals, other organizations, or the Nation; and considering the results from system and organizational risk assessments. CNSSI 1253 provides guidance on control baselines for national security systems.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** None. **Federal**: FIPS 199, 200; NIST SP 800-30, 800-37, 800-39, 800-53B, 800-60-1, 800-60-2, 800-160-1; CNSSI 1253.	PL-2, PL-11, RA-2, RA-3, SA-8.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Security and privacy planning policy; procedures addressing system security and privacy plan development and implementation; procedures addressing system security and privacy plan reviews and updates; system design documentation; system architecture and configuration documentation; system categorization decision; information types stored, transmitted, and processed by the system; system element/component information; stakeholder needs analysis; list of security and privacy requirements allocated to the system, system elements, and environment of operation; list of contractual requirements allocated to external providers of the system or system element; business impact analysis or criticality analysis; risk assessments; risk management strategy; organizational security and privacy policy; federal or organization-approved or mandated baselines or overlays; system security plan; privacy plan; other relevant documents or records

Interview: Organizational personnel with security and privacy planning and plan implementation responsibilities; organizational personnel with information security and privacy responsibilities; organizational personnel with responsibility for organizational risk management activities.

PL-11: BASELINE TAILORING

Baseline(s): N/A	Overlay(s): N/A

CONTROL REQUIREMENTS

Tailor the selected control baseline by applying specified tailoring actions.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Document tailored baselines in the System Security Plan (SSP), including rationale for tailoring and any security-relevant sources.

a. NOTE: Potential inputs for baseline tailoring include, but are not limited to, risk assessment results, system and component inventories, system criticality, business and privacy impact analysis, risk management strategy, and partnership agreements. Tailored baselines for a system may not be less stringent than the DFPS Information Security Minimum Baseline Standard.

SUPPLEMENTAL GUIDANCE

Control baselines are predefined sets of controls specifically assembled to address the protection needs of a group, organization, or community of interest. Controls are chosen for baselines to either satisfy mandates imposed by laws, executive orders, directives, regulations, policies, standards, and guidelines or address threats common to all users of the baseline under the assumptions specific to the baseline. Baselines represent a starting point for the protection of individuals' privacy, information, and information systems with subsequent tailoring actions to manage risk in accordance with mission, business, or other constraints (see PL-11). Federal control baselines are provided in SP 800-53B. The selection of a control baseline is determined by the needs of stakeholders. Stakeholder needs consider mission and business requirements as well as mandates imposed by applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. For example, the control baselines in SP 800-53B are based on the requirements from FISMA and PRIVACT. The requirements, along with the NIST standards and guidelines implementing the legislation, direct organizations to select one of the control baselines after the reviewing the information types and the information that is processed, stored, and transmitted on the system; analyzing the potential adverse impact of the loss or compromise of the information or system on the organization's operations and assets, individuals, other organizations, or the Nation; and considering the results from system and organizational risk assessments. CNSSI 1253 provides guidance on control baselines for national security systems.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Information Security Minimum Baseline Standard. **State:** None. **Federal**: FIPS 199, 200; NIST SP 800-30, 800-37, 800-39, 800-53B, 800-60-1, 800-60-2, 800-160-1; CNSSI 1253.	PL-2, PL-11, RA-2, RA-3, SA-8.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Security and privacy planning policy; procedures addressing system security and privacy plan development and implementation; system design documentation; system categorization decision; information types stored, transmitted, and processed by the system; system element/component information; stakeholder needs analysis; list of security and privacy requirements allocated to the system, system elements, and environment of operation; list of contractual requirements allocated to external providers of the system or system element; business impact analysis or criticality analysis; risk assessments; risk management strategy; organizational security and privacy policy; federal or organization-approved or mandated baselines or overlays; baseline tailoring rationale; system security plan; privacy plan; records of system security and privacy plan reviews and updates; other relevant documents or records.

Interview: Organizational personnel with security and privacy planning and plan implementation responsibilities; organizational personnel with information security and privacy responsibilities.

(PM) PROGRAM MANAGEMENT

The PM control family applies to the DFPS cybersecurity program. It includes a critical infrastructure plan, information security program plan, a plan of action milestones and processes, a risk management strategy, and enterprise architecture. The PM family provides controls for information security programs required by Federal Information Security Management Act (FISMA). This family provides security controls at the organization level rather than the information system level.

The intended audience for this Control includes, but is not limited to, the DFPS Chief Information Security Officer (CISO) and/or their designee and the Office of Information Security.

PM-01: INFORMATION SECURITY PROGRAM PLAN

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Develop and disseminate an organization-wide information security program plan that:
   1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;
   2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
   3. Reflects the coordination among organizational entities responsible for information security; and
   4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;

b. Review and update the organization-wide information security program plan annually and following major changes to legislation or security requirements; and

c. Protect the information security program plan from unauthorized disclosure and modification.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS must have an information resources security program consistent with the standards described in PM-1, and the DFPS Commissioner is responsible for the protection of information resources. [Source: DIR Control Standards Catalog PM-1]

Std.02 — The DFPS Commissioner or his/her designated representative(s) shall ensure that senior agency officials support the Information Security Officer in developing, at least annually, a report on agency information security program, as specified in 1 TAC 202.21(b)(11) and 202.23(a). [Source: 1 TAC 202.20(5)]

Std.03 —

a. Agency Program. DFPS shall develop, document, and implement an agency-wide information security program, approved by the agency head under 1 TAC 202.20, that includes protections, based on risk, for all information and information resources owned, leased, or under the custodianship of any department, operating unit, or employee of the agency including outsourced resources to another agency, contractor, or other source (e.g., cloud computing). The program shall include:

   1. Periodic assessments of the risk and impact that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency;

   2. Policies, controls, standards, and procedures that:
      a) Are based on the risk assessments required by 1 TAC 202.25;
      b) Cost-effectively reduce information security risks to a level acceptable to the agency head;
      c) Ensure that information security is addressed throughout the life cycle of each agency information resource; and
      d) Ensure compliance with:
         (i) The requirements of 1 TAC 202.24;
         (ii) Minimally acceptable system configuration requirements, as determined by the agency; and
         (iii) The control catalog published by DIR;

   3. Strategies to address risk to High-Impact information resources;

   4. Plans for providing information security for networks, facilities, and systems or groups of information systems, based on risk;

   5. A process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency; and

   6. A process to justify, grant and document any exceptions to specific program requirements in accordance with requirements and processes defined in 1 TAC 202. [Source: 1 TAC 202.24(a)]; and

b. Information Security Plan.

   1. Each state agency shall develop, and periodically update, an information security plan for protecting the security of the agency's information.
   2. In developing the plan, the state agency shall:
      a) Consider any vulnerability report prepared under Section 2054.077 for the agency;
      b) Incorporate the network security services provided by the department to the agency under Chapter 2059;
      c) Identify and define the responsibilities of agency staff who produce, access, use, or serve as custodians of the agency's information;
      d) Identify risk management and other measures taken to protect the agency's information from unauthorized access, disclosure, modification, or destruction;
      e) Include:
         (i) The best practices for information security developed by the department; or
         (ii) A written explanation of why the best practices are not sufficient for the agency's security; and
      f) Omit from any written copies of the plan information that could expose vulnerabilities in the agency's network or online systems.

3. Not later than June 1 of each even-numbered year, each state agency shall submit a copy of the agency's information security plan to the department. Subject to available resources, the department may select a portion of the submitted security plans to be assessed by the department in accordance with department rules.
4. Each state agency's information security plan is confidential and exempt from disclosure under Chapter 552.
5. Each state agency shall include in the agency's information security plan a written document that is signed by the head of the agency, the chief financial officer, and each executive manager designated by the state agency and states that those persons have been made aware of the risks revealed during the preparation of the agency's information security plan. [Source: TX Govt. Code 2054.133]

Std.04 — The DFPS Commissioner or his/her designated representative(s) shall review and approve at least annually the agency information security program required under 1 TAC 202.24. [Source: 1 TAC 202.20(7)]

Std.05 — The DFPS Chief Information Security Officer shall be responsible for developing and maintaining an agency-wide information security plan as required by Sec. 2054.133, Texas Government Code. [Source: 1 TAC 202.21(b)(1)]

Std.06 — The DFPS Chief Information Security Officer shall be responsible for reporting, at least annually, to the DFPS Commissioner the status and effectiveness of security controls. [Source: 1 TAC 202.21(b)(11)]

Std.07 — The DFPS Chief Information Security Officer shall be responsible for informing the parties in the event of noncompliance with 1 TAC 202 and/or with the agency's information security policies. [Source: 1 TAC 202.21(b)(12)]

Std.08 — DFPS shall submit to the Department of Information Resources a Biennial Information Security Plan, in accordance with Sec. 2054.133, Texas Government Code. [Source: 1 TAC 202.23(b)(3)]

Std.09 — A review of DFPS information security program for compliance with the standards in the Security Control Standards Catalog will be performed at least biennially, based on business risk management decisions, by individual(s) independent of the information security program and designated by the DFPS Commissioner or his or her designated representative(s). [Source: 1 TAC 202.26(c)]

Std.10 — The DFPS Chief Information Security Officer shall prepare or have prepared a report, including an executive summary of the findings of the biennial report, not later than October 15 of each even-numbered year, assessing the extent to which a computer, a computer program, a computer network, a computer system, a printer, an interface to a computer system, including mobile and peripheral devices, computer software, or data processing of the agency or of a contractor of the agency is vulnerable to unauthorized access or harm, including the extent to which the agency's or contractor's electronically stored information is vulnerable to alteration, damage, erasure, or inappropriate use. [Source: TX Govt. Code 2054.077(b)]

Std.11 — Separate from the executive summary described by TX Govt. Code 2057.077(b), DFPS shall prepare a summary of the agency's vulnerability report that does not contain any information the release of which might compromise the security of the agency's or agency contractor's computers, computer programs, computer networks, computer systems, printers, interfaces to computer systems, including mobile and peripheral devices, computer software, data processing, or electronically stored information. The summary is available to the public on request. [Source: TX Govt. Code 2054.077(e)]

Std.12 — If the Department of Information Resources (DIR) provides network security services for DFPS, DIR is responsible for network security from external threats for the agency. Network security management for DFPS regarding internal threats remains the responsibility of the agency. [Source: TX Govt. Code 2059.056]

SUPPLEMENTAL GUIDANCE

An information security program plan is a formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements. An information security program plan can be represented in a single document or compilations of documents. Privacy program plans and supply chain risk management plans are addressed separately in PM-18 and SR-02, respectively.

An information security program plan documents implementation details about program management and common controls. The plan provides sufficient information about the controls (including specification of parameters for assignment and selection operations, explicitly or by reference) to enable implementations that are unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended. Updates to information security program plans include organizational changes and problems identified during plan implementation or control assessments.

Program management controls may be implemented at the organization level or the mission or business process level and are essential for managing the organization's information security program. Program management controls are distinct from common, system-specific, and hybrid controls because program management controls are independent of any particular system. Together, the individual system security plans and the organization-wide information security program plan provide complete coverage for the security controls employed within the organization.

Common controls available for inheritance by organizational systems are documented in an appendix to the organization's information security program plan unless the controls are included in a separate security plan for a system. The organization-wide information security program plan indicates which separate security plans contain descriptions of common controls.

Events that may precipitate an update to the information security program plan include, but are not limited to, organization-wide assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Information Security Program Policy. **State:** 1 TAC 202.20(5), 1 TAC 202.20(7), 1 TAC 202.21(b)(1), 1 TAC 202.21(b)(11), 1 TAC 202.21(b)(12), 1 TAC 202.23(b)(3), 1 TAC 202.26(c); TX Govt. Code 2054.077, TX Govt. Code 2054.133; DIR Security Control Standards Catalog **Federal**: FISMA; OMB A-130; NIST SP 800-37, 800-39; FBI CJIS CSP v5.9	PL-2, PM-18, PM-30, RA-9, SI-12, SR-2.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Information security program plan; procedures addressing program plan development and implementation; procedures addressing program plan reviews and updates; procedures addressing coordination of the program plan with relevant entities; procedures for program plan approvals; records of program plan reviews and updates; other relevant documents or records.

Interview: Organizational personnel with information security program planning and plan implementation responsibilities; organizational personnel with information security responsibilities.

Test: Organizational processes for information security program plan development, review, update, and approval; automated mechanisms supporting and/or implementing the information security program plan

PM-02: SENIOR INFORMATION SECURITY OFFICER

Priority: P1	
Baseline(s): Low, Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization appoints a senior agency information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — The DFPS Commissioner or his or her designated representative(s) shall designate an information security officer to administer the state organization information security program. [Source: DIR Control Standards Catalog PM-2]

Std.02 — The DFPS Commissioner or his/her designated representative(s) shall designate an Information Security Officer who has the explicit authority and the duty to administer the information security requirements of 1 TAC 202 agency wide. [Source: 1 TAC 202.20(1)]

Std.03 — DFPS's Information Security Officer shall report to executive level management; have authority for information security for the entire agency; possess training and experience required to administer the functions described in 1 TAC 202; and, whenever possible, have information security duties as the primary duty. [Source: 1 TAC 202.21(a)]

Std.04 — The DFPS Chief Information Security Officer shall be responsible for developing and maintaining information security policies and procedures that address the requirements of 1 TAC 202 and the agency's information security risks; working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks; providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities under 1 TAC 202. [Source: 1 TAC 202.21(b)(2, 3, 5)]

SUPPLEMENTAL GUIDANCE

The senior agency information security officer is an organizational official. For federal agencies (as defined by applicable laws, executive orders, regulations, directives, policies, and standards), this official is the senior agency information security officer. Organizations may also refer to this official as the senior information security officer or chief information security officer.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Information Security Program Policy. **State:** 1 TAC 202.20(1), 1 TAC 202.21(a), 1 TAC 202.21(b)(2, 3, 5); TX Govt. Code 2054.136; DIR Security Control Standards Catalog. **Federal**: OMB M-17-25; NIST SP 800-37, 800-39, 800-181.	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Information security program plan; procedures addressing program plan development and implementation; procedures addressing program plan reviews and updates; procedures addressing coordination of the program plan with relevant entities; other relevant documents or records.

Interview: Organizational personnel with information security program planning and plan implementation responsibilities; senior information security officer; organizational personnel with information security responsibilities.

PM-03: INFORMATION SECURITY RESOURCES

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization:

a. Include the resources needed to implement the information security and privacy programs in capital planning and investment requests and document all exceptions to this requirement;

b. Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, executive orders, directives, policies, regulations, standards; and

c. Make available for expenditure, the planned information security and privacy resources.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — The DFPS Commissioner or his or her designated representative(s) shall allocate resources for ongoing information security remediation, implementation, and compliance activities that reduce risk to a level acceptable to the DFPS Commissioner. [Source: 1 TAC 202.20(2)]

Std.02 — The DFPS Chief Information Security Officer shall report, at least annually, to the DFPS Commissioner on the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the requirements of 1 TAC 202 and agency information security requirements and requests. [Source: 1 TAC 202.23(a)(3)]

SUPPLEMENTAL GUIDANCE

Organizations consider establishing champions for information security and privacy and, as part of including the necessary resources, assign specialized expertise and resources as needed. Organizations may designate and empower an Investment Review Board or similar group to manage and provide oversight for the information security and privacy aspects of the capital planning and investment control process.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Information Security Program Policy. **State:** 1 TAC 202.20(2), 1 TAC 202.23(a)(3); DIR Security Control Standards Catalog. **Federal**: OMB M-17-25.	PM-4, SA-2.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Information security program plan; Exhibit 300; Exhibit 53; business cases for capital planning and investment; procedures for capital planning and investment; documentation of exceptions to capital planning requirements; other relevant documents or records.

Interview: Organizational personnel with information security program planning responsibilities; organizational personnel responsible for capital planning and investment; organizational personnel with information security responsibilities.

Test: Organizational processes for capital planning and investment; organizational processes for business case, Exhibit 300, and Exhibit 53 development; automated mechanisms supporting the capital planning and investment process.

PM-04: PLAN OF ACTION AND MILESTONES PROCESS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization:

a. Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated organizational systems:

1. Are developed and maintained;
2. Document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and
3. Are reported in accordance with established reporting requirements.

b. Review plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS must develop and update a plan of action and milestone process for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct deficiencies noted during the assessment of the security controls in order to reduce or eliminate known vulnerabilities in the system. [Source: DIR Control Standards Catalog PM-4]

Std.02 — An agency-wide information security program must be approved by the agency head and include a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency. [Source: 1 TAC 202.24(a)(5)]

SUPPLEMENTAL GUIDANCE

The plan of action and milestones is a key organizational document and is subject to reporting requirements established by the Office of Management and Budget. Organizations develop plans of action and milestones with an organization-wide perspective, prioritizing risk response actions and ensuring consistency with the goals and objectives of the organization. Plan of action and milestones updates are based on findings from control assessments and continuous monitoring activities. There can be multiple plans of action and milestones corresponding to the information system level, mission/business process level, and organizational/governance level. While plans of action and milestones are required for federal organizations, other types of organizations

can help reduce risk by documenting and tracking planned remediations. Specific guidance on plans of action and milestones at the system level is provided in CA-05.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Information Security Program Policy. **State:** 1 TAC 202.24(a)(5); DIR Security Control Standards Catalog. **Federal**: Privacy Act; OMB A-130; NIST SP 800-37.	CA-5, CA-7, PM-3, RA-7, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Information security program plan; Exhibit 300; Exhibit 53; business cases for capital planning and investment; procedures for capital planning and investment; documentation of exceptions to capital planning requirements; other relevant documents or records.

Interview: Organizational personnel with information security program planning responsibilities; organizational personnel responsible for capital planning and investment; organizational personnel with information security responsibilities.

Test: Organizational processes for capital planning and investment; organizational processes for business case, Exhibit 300, and Exhibit 53 development; automated mechanisms supporting the capital planning and investment process.

PM-05: INFORMATION SYSTEM INVENTORY

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization develop and update at least annually an inventory of organizational systems.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS must develop and maintain an inventory of its information systems. [Source: DIR Control Standards Catalog PM-5]

Std.02 — The DFPS Chief Information Security Officer shall be responsible for reviewing the agency's inventory of information systems and related ownership and responsibilities. [Source: 1 TAC 202.21(b)(7)]

Std.03 — Not later than March 31 of each even-number year, DFPS shall complete a review of the operational aspects of the agency's information resources that includes:

a. An inventory of the agency's major information systems, as defined by Section 2054.008, and other operational and logistical components related to deployment of information resources as prescribed by the Texas Department of Information Resources (DIR).

b. An inventory of the agency's major databases and applications.

c. Analysis of how information systems, components, databases, applications, and other information system resources have been deployed by the agency in support of:

1. Applicable achievement goals established under Section 2056.006 and the state strategic plan adopted under Section 2056.009;
2. The state strategic plan for information resources; and
3. The agency's business objectives, mission, and goals. [Source: TX Govt. Code 2054.0965(a)]

Std.04 — All DFPS information systems must be registered when the proposed system is funded. The system inventory must identify the information owner, information custodian, and any requirements outlined in RA-02.

Std.05 — The Information Owner must annually review and validate the accuracy of information systems information for which they are the owner.

SUPPLEMENTAL GUIDANCE

This control addresses the inventory requirements in FISMA. OMB A-130 provides guidance on developing information systems inventories and associated reporting requirements. For specific information system inventory reporting requirements, organizations consult OMB annual FISMA reporting guidance.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** 1 TAC 202.21(b)(7); TX Govt. Code 2054.068, TX Govt. Code 2054.0965; DIR Security Control Standards Catalog. **Federal**: NIST IR 8062; OMB A-130	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Information security program plan; system inventory; procedures addressing system inventory development and maintenance; OMB FISMA reporting guidance; other relevant documents or records.

Interview: Organizational personnel with information security program planning and plan implementation responsibilities; organizational personnel responsible for developing and maintaining the system inventory; organizational personnel with information security responsibilities.

Test: Organizational processes for system inventory development and maintenance; automated mechanisms supporting the system inventory.

PM-05(01): INVENTORY OF PERSONALLY IDENTIFIABLE INFORMATION

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization establishes, maintains, and updates at least annually an inventory of all systems, applications, and projects that process personally identifiable information.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Classify all DFPS data in accordance with the DFPS Data Classification Policy.

Std.02 — Document, in inventories and System Security Plans (SSPs), which elements of personally identifiable information (PII) the system processes.

SUPPLEMENTAL GUIDANCE

An inventory of systems, applications, and projects that process personally identifiable information supports the mapping of data actions, providing individuals with privacy notices, maintaining accurate personally identifiable information, and limiting the processing of personally identifiable information when such information is not needed for operational purposes. Organizations may use this inventory to ensure that systems only process the personally identifiable information for authorized purposes and that this processing is still relevant and necessary for the purpose specified therein.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Data Classification Policy. **State:** DIR Security Control Standards Catalog. **Federal**: NIST IR 8062.	AC-3, CM-8, CM-12, CM-13, PL-8, PM-22, PT-3, PT-5, SI-12, SI-18.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Procedures addressing system inventory development, maintenance, and updates; OMB FISMA reporting guidance; privacy program plan; information security program plan; personally identifiable information processing policy; system inventory; personally identifiable information inventory; data mapping documentation; other relevant documents or records.

Interview: Procedures addressing system inventory development, maintenance, and updates; OMB FISMA reporting guidance; privacy program plan; information security program plan; personally identifiable information processing policy; system inventory; personally identifiable information inventory; data mapping documentation; other relevant documents or records.

Test: Organizational processes for system inventory development, maintenance, and updates; automated mechanisms supporting the system inventory.

PM-06: INFORMATION SECURITY MEASURES OF PERFORMANCE

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization develops, monitors, and reports on the results of information security and privacy measures of performance.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS must develop, monitor, and report on the results of information security measures of performance. [Source: DIR Control Standards Catalog PM-6]

Std.02 — The DFPS Chief Information Security Officer shall be responsible for reporting, at least annually, to the DFPS Commissioner the status and effectiveness of security controls. [Source: 1 TAC 202.21(b)(11)]

Std.03 — The DFPS Chief Information Security Officer shall report, at least annually, to the DFPS Commissioner on the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the requirements of 1 TAC 202 and the effectiveness of current information security program and status of key initiatives. [Source: 1 TAC 202.23(a)(1)]

Std.04 — Before issuing a vendor solicitation for a project or major project, DFPS must develop, consistent with DIR guidelines, a procurement plan with anticipated service levels and performance standards for each vendor. [Source: TX Govt. Code 2054.305(1)].

SUPPLEMENTAL GUIDANCE

Measures of performance are outcome-based metrics used by an organization to measure the effectiveness or efficiency of the information security program and the security controls employed in support of the program.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** 1 TAC 202.23(a)(1); DIR Security Control Standards Catalog. **Federal**: OMB A-130; NIST SP 800-37, 800-39, 800-55, 800-137.	CA-7, PM-9.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Information security program plan; privacy program plan; information security measures of performance; privacy measures of performance; procedures addressing the development, monitoring, and reporting of information security and privacy measures of performance; risk management strategy; other relevant documents or records.

Interview: Organizational personnel with information security and privacy program planning and plan implementation responsibilities; organizational personnel responsible for developing, monitoring, and reporting information security and privacy measures of performance; organizational personnel with information security and privacy responsibilities.

Test: Organizational processes for developing, monitoring, and reporting information security and privacy measures of performance; automated mechanisms supporting the development, monitoring, and reporting of information security and privacy measures of performance.

PM-07: ENTERPRISE ARCHITECTURE

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — The agency's enterprise information security architecture must be aligned with Federal, State, Local and agency data security and privacy requirements. [Source: Texas Cybersecurity Framework].

Std.02 — The Information Security Program must, using a roadmap and emerging technology process, stay abreast of the continued evolution of security solutions, processes, and technology to identify continuous, ongoing ways to deliver technology and information securely. [Source: Texas Cybersecurity Framework].

Std.03 — Ensure the enterprise architecture includes models and transition plans and aligns with the agency Information Security Plan.

SUPPLEMENTAL GUIDANCE

The integration of security and privacy requirements and controls into the enterprise architecture helps to ensure that security and privacy considerations are addressed throughout the system development life cycle and are explicitly related to the organization's mission and business processes. The process of security and privacy requirements integration also embeds into the enterprise architecture and the organization's security and privacy architectures consistent with the organizational risk management strategy. For PM- 07, security and privacy architectures are developed at a system-of-systems level, representing all organizational systems. For PL-08, the security and privacy architectures are developed at a level that represents an individual system. The system-level architectures are consistent with the security and privacy architectures defined for the organization. Security and privacy requirements and control integration are most effectively accomplished through the rigorous application of the Risk Management Framework and supporting security standards and guidelines.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** 1 TAC 202.23(a)(1); DIR Security Control Standards Catalog. **Federal**: OMB A-130; NIST SP 800-37, 800-39, 800-160-1, 800-160-2.	AU-6, PL-2, PL-8, PM-11, RA-2, SA-3, SA-8, SA-17.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Information security program plan; privacy program plan; enterprise architecture documentation; procedures addressing enterprise architecture development; results of risk assessments of enterprise architecture; other relevant documents or records.

Interview: Organizational personnel with information security and privacy program planning and plan implementation responsibilities; organizational personnel responsible for developing enterprise architecture; organizational personnel responsible for risk assessments of enterprise architecture; organizational personnel with information security and privacy responsibilities.

Test: Organizational processes for enterprise architecture development; automated mechanisms supporting the enterprise architecture and its development.

PM-08: CRITICAL INFRASTRUCTURE PLAN

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Identify all agency assets, business processes, and resources that meet the definition of critical infrastructure and document that status in applicable System Security Plans (SSPs) and COOPs.

SUPPLEMENTAL GUIDANCE

Protection strategies are based on the prioritization of critical assets and resources. The requirement and guidance for defining critical infrastructure and key resources and for preparing an associated critical infrastructure protection plan are found in applicable laws, executive orders, directives, policies, regulations, standards, and guidelines.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** TX Govt. Code 2054.069; DIR Security Control Standards Catalog **Federal**: EO 13636; OMB A-130; HSPD 7; DHS National Infrastructure Protection Plan.	CP-2, CP-4, PE-18, PL-2, PM-9, PM-11, PM-18, RA-3, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Information security program plan; privacy program plan; critical infrastructure and key resources protection plan; procedures addressing the development, documentation, and updating of the critical infrastructure and key resources protection plan; HSPD 7; National Infrastructure Protection Plan; other relevant documents or records.

Interview: Organizational personnel with information security and privacy program planning and plan implementation responsibilities; organizational personnel responsible for developing, documenting, and updating the critical infrastructure and key resources protection plan; organizational personnel with information security and privacy responsibilities.

Test: Organizational processes for developing, documenting, and updating the critical infrastructure and key resources protection plan; automated mechanisms supporting the development, documentation, and updating of the critical infrastructure and key resources protection plan.

PM-09: RISK MANAGEMENT STRATEGY

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization:

a. Develops a comprehensive strategy to manage:
   1. Security risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of organizational systems; and
   2. Privacy risk to individuals resulting from the authorized processing of personally identifiable information;
b. Implement the risk management strategy consistently across the organization; and
c. Review and update the risk management strategy annually or as required, to address organizational changes.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — The DFPS risk management strategy must align with NIST's Risk Management Framework and includes the DFPS Information Security and Privacy Controls Standards Catalog.

Std.02 — Information Security Plan:

a. Each state agency shall develop, and periodically update, an information security plan for protecting the security of the agency's information. [Source: TX Govt. Code 2054.133(a)]

   1. Within this plan, DFPS shall identify risk management and other measures taken to protect the agency's information from unauthorized access, disclosure, modification, or destruction. [Source: TX Govt. Code 2054.133(b)(4)]

b. Not later than June 1 of each even-numbered year, DFPS shall submit a copy of the agency's information security plan to the Department of Information Resources. [Source: TX Govt. Code 2054.133(c)]

c. DFPS information security plan is confidential and exempt from disclosure under Chapter 552. [Source: TX Govt. Code 2054.133(d)]

d. DFPS shall include in the agency's information security plan a written document that is signed by the DFPS Commissioner and each executive manager designated by the agency and states that those persons have been made aware of the risks revealed during the preparation of the agency's information security plan. [Source: TX Govt. Code 2054.133(e)]
   1. Omit from any written copies of the plan information that could expose vulnerabilities in the agency's network or online systems. [Source: TX Govt. Code 2054.133(b)(6)]

Std.03 — DFPS Information Security Risk Management Reporting:

a. DFPS's Chief Information Security Officer shall report, at least annually, to the DFPS Commissioner the status and effectiveness of security controls. [Source: 1 TAC 202.21(b)(11)]

b. The DFPS Chief Information Security Officer shall report, at least annually, to the DFPS Commissioner on residual risks identified by the agency risk management process. [Source: 1 TAC 202.23(a)(2)]

c. Approval of the security risk acceptance, transference, or mitigation decision shall be the responsibility of the DFPS Commissioner for all systems identified with a residual High Risk. [Source: 1 TAC 202.25(4)(B)]

Std.04 — Vulnerability Reports:

a. DFPS's Chief Information Security Officer shall prepare or have prepared a report, including an executive summary of the findings of the biennial report, not later than October 15 of each even-numbered year, assessing the extent to which a computer, a computer program, a computer network, a computer system, a

printer, an interface to a computer system, including mobile and peripheral devices, computer software, or data processing of the agency or of a contractor of the agency is vulnerable to unauthorized access or harm, including the extent to which the agency's or contractor's electronically stored information is vulnerable to alteration, damage, erasure, or inappropriate use. [Source: TX Govt. Code 2054.077(b)]

b. Except as provided by TX Govt. Code 2054.077, a vulnerability report and any information or communication prepared or maintained for use in the preparation of a vulnerability report is confidential and is not subject to disclosure under Chapter 552. [Source: TX Govt. Code 2054.077(c)]

c. Separate from the executive summary described by TX Govt. Code 2057.077(b), DFPS shall prepare a summary of the agency's vulnerability report that does not contain any information the release of which might compromise the security of the agency's or agency contractor's computers, computer programs, computer networks, computer systems, printers, interfaces to computer systems, including mobile and peripheral devices, computer software, data processing, or electronically stored information. The summary is available to the public on request. [Source: TX Govt. Code 2054.077(e)]

SUPPLEMENTAL GUIDANCE

An organization-wide risk management strategy includes an expression of the security and privacy risk tolerance for the organization, security and privacy risk mitigation strategies, acceptable risk assessment methodologies, a process for evaluating security and privacy risk across the organization with respect to the organization's risk tolerance, and approaches for monitoring risk over time. The senior accountable official for risk management (agency head or designated official) aligns information security management processes with strategic, operational, and budgetary planning processes. The risk executive

function, led by the senior accountable official for risk management, can facilitate consistent application of the risk management strategy organization wide. The risk management strategy can be informed by security and privacy risk-related inputs from other sources, both internal and external to the organization, to ensure that the strategy is broad-based and comprehensive. The supply chain risk management strategy described in PM-30 can also provide useful inputs to the organization-wide risk management strategy.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** 1 TAC 202.21(b)(11), 1 TAC 202.23(a)(2), 1 TAC 202.25(4)(B); TX Govt. Code 2054.077; DIR Security Control Standards Catalog. **Federal**: OMB A-130; NIST SP 800-30, 800-37, 800-39, 800-161; NIST IR 8023.	AC-1, AU-1, AT-1, CA-1, CA-2, CA-5, CA-6, CA-7, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PL-2, PM-2, PM-8, PM-18, PM-28, PM-30, PS-1, PT-1, PT-2, PT-3, RA-1, RA-3, RA-9, SA-1, SA-4, SC-1, SC-38, SI-1, SI-12, SR-1, SR-2.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Information security program plan; privacy program plan; risk management strategy; supply chain risk management strategy; procedures addressing the development, implementation, review, and update of the risk management strategy; risk assessment results relevant to the risk management strategy; other relevant documents or records.

Interview: Organizational personnel with information security and privacy program planning and plan implementation responsibilities; organizational personnel responsible for the development, implementation, review, and update of the risk management strategy; organizational personnel with information security and privacy responsibilities.

Test: Organizational processes for the development, implementation, review, and update of the risk management strategy; automated mechanisms supporting the development, implementation, review, and update of the risk management strategy.

PM-10: SECURITY AUTHORIZATION PROCESS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization:

a. Manage the security and privacy state of organizational systems and the environments in which those systems operate through authorization processes;

b. Designate individuals to fulfill specific roles and responsibilities within the organizational risk management process; and

c. Integrate the authorization processes into an organization-wide risk management program.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — The Authorizing Official (AO) formally assumes responsibility for operating an information system at an acceptable level of risk. No system shall be deployed to an operational state in a production environment without an Authorization to Operate approved by an AO.

a. The Authorizing Official should ensure:

1. New information processing assets (internal to the organization or via a service provided by a third party) have appropriate user management authorization of their purpose and use, and authorization is also obtained from the manager responsible for maintaining the local information system security environment to ensure that all relevant security policies and requirements are met;

2. Information assets have appropriate security measures commensurate with the type of information they will store, process, or transmit;

3. The assets comply with all applicable laws, regulations, standards, policies, and other applicable frameworks including the Texas Cybersecurity Risk Framework;

4. Hardware and software are checked to ensure that they are compatible with other system components; and

5. Necessary controls for the use of personal or privately-owned information processing equipment (e.g., laptops, home-computers, or hand-held devices) for processing business information, which may introduce new vulnerabilities, are identified, and implemented. [Source: Hitrust CSF 05.d Authorization Process for Information Assets and Facilities]

SUPPLEMENTAL GUIDANCE

Authorization processes for organizational systems and environments of operation require the implementation of an organization-wide risk management process and associated security and privacy standards and guidelines. Specific roles for risk management processes include a risk executive (function) and designated authorizing officials for each organizational system and common control provider. The authorization processes for the organization are integrated with continuous monitoring processes to facilitate ongoing understanding and acceptance of security and privacy risks to organizational operations, organizational assets, individuals, other organizations, and the Nation.

REFERENCES	RELATED CONTROLS

Agency: DFPS Information Security Policy. **State:** Texas Cybersecurity Framework; DIR Security Control Standards Catalog. **Federal**: NIST SP 800-37, 800-39, 800-181	CA-6, CA-7, PL-2.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Information security program plan; privacy program plan; procedures addressing management (i.e., documentation, tracking, and reporting) of the authorization process; assessment, authorization, and monitoring policy; assessment, authorization, and monitoring procedures; system authorization documentation; lists or other documentation about authorization process roles and responsibilities; risk assessment results relevant to the authorization process and the organization-wide risk management program; organizational risk management strategy; other relevant documents or records.

Interview: Organizational personnel with information security and privacy program planning and plan implementation responsibilities; organizational personnel responsible for management of the authorization process; organizational personnel with information security and privacy responsibilities.

Test: Organizational processes for authorization; automated mechanisms supporting the authorization process.

PM-11: MISSION/BUSINESS PROCESS DEFINITION

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization:

a. Define organizational mission and business processes with consideration for information security and privacy and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and

b. Determine information protection and personally identifiable information processing needs arising from the defined mission and business processes; and

c. Review and revise the mission and business processes at least annually and whenever changes to the environment of operation (including threats, infrastructures, and legislation) warrant.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Priorities for organizational mission, objectives, and activities are established and communicated [Source: Cybersecurity Framework ID.BE-3]

Std.02 — Document mission and business process priorities in applicable System Security Plans (SSPs) and COOPs, either as Cybersecurity Framework Profiles or in another approved format. [Source: Hitrust CSF 05.d Authorization Process for Information Assets and Facilities]

SUPPLEMENTAL GUIDANCE

Protection needs are technology-independent capabilities that are required to counter threats to organizations, individuals, systems, and the Nation through the compromise of information (i.e., loss of confidentiality, integrity, availability, or privacy). Information protection and personally identifiable information processing needs are derived from the mission and business needs defined by organizational stakeholders, the mission and business processes designed to meet those needs, and the organizational risk management strategy. Information protection and personally identifiable information processing needs determine the required controls for the organization and the systems. Inherent to defining protection and personally identifiable information processing needs is an understanding of the adverse impact that could result if a compromise or breach of information occurs. The categorization process is used to make such potential impact determinations. Privacy risks to individuals can arise from the compromise of personally identifiable information, but they can also arise as unintended consequences or a byproduct of the processing of personally identifiable information at any stage of the information life cycle. Privacy risk assessments are used to prioritize the risks that are created for individuals from system processing of personally identifiable information. These risk assessments enable the selection of the required privacy controls for the organization and systems. Mission and business process definitions and the associated protection requirements are documented in accordance with organizational policies and procedures.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; FIPS 199; NIST SP 800-39, 800-60-1, 800-60-2, 800-160-1; NITP12	CP-2, PL-2, PM-7, PM-8, RA-2, RA-3, RA-9, SA-2.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Information security program plan; privacy program plan; risk management strategy; procedures for determining mission and business protection needs; information security and privacy risk assessment results relevant to the determination of mission and business protection needs; personally identifiable information processing policy; personally identifiable information inventory; other relevant documents or records.

Interview: Organizational personnel with information security and privacy program planning and plan implementation responsibilities; organizational personnel responsible for enterprise risk management; organizational personnel responsible for determining information protection needs for mission and business processes; organizational personnel with information security and privacy responsibilities.

Test: Organizational processes for defining mission and business processes and their information protection needs.

PM-12: INSIDER THREAT PROGRAM

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Include insider threat in the incident response plan established in accordance with IR-08, including mitigation of risk, monitoring, response, and training.

Std.02 —

a. Information security events shall be reported through appropriate communications channels as quickly as possible. All employees, contractors and third-party users shall be made aware of their responsibility to report any information security events as quickly as possible. [Source: Hitrust 11.a Reporting Information Security Events]

b. Information Security Training for employees and contractors must include content on insider threat including instructions on reporting.

SUPPLEMENTAL GUIDANCE

Organizations handling classified information are required, under Executive Order 13587 and the National Policy on Insider Threat, to establish insider threat programs. The standards and guidelines that apply to insider threat programs in classified environments can also be employed effectively to improve the security of Controlled Unclassified Information in non-national security systems. Insider threat programs include security controls to detect and prevent malicious insider activity through the centralized integration and analysis of both technical and non-technical information to identify potential insider threat concerns. A senior organizational official is designated by the department/agency head as the responsible individual to implement and provide oversight for the program. In addition to the centralized integration and analysis capability, insider threat programs as a minimum, prepare department/agency insider threat policies and implementation plans, conduct host-based user monitoring of individual employee activities on government-owned classified computers, provide insider threat awareness training to employees, receive access to information from all offices within the department/agency (e.g., human resources, legal, physical security, personnel security, information technology, information system security, and law enforcement) for insider threat analysis, and conduct self-assessments of department/agency insider threat posture.

Insider threat programs can leverage the existence of incident handling teams' organizations may already have in place, such as computer security incident response teams. Human resources records are especially important in this effort, as there is compelling evidence to show that some types of insider crimes are often preceded by nontechnical behaviors in the workplace (e.g., ongoing patterns of disgruntled behavior and conflicts with coworkers and other colleagues). These precursors can better inform and guide organizational officials in more focused, targeted monitoring efforts. The participation of a legal team is important to ensure that all monitoring activities are performed in accordance with appropriate legislation, directives, regulations, policies, standards, and guidelines.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: EO 13587; ODNI National Insider Threat Policy.	AC-6, AT-2, AU-6, AU-7, AU-10, AU-12, AU-13, CA-7, IA-4, IR-4, MP-7, PE-2, PM-16, PS-3, PS-4, PS-5, PS-7, PS-8, SC-7, SC-38, SI-4, PM-14.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Organizational personnel with information security and privacy program planning and plan implementation responsibilities; organizational personnel responsible for the insider threat program; members of

the cross-discipline insider threat incident handling team; legal counsel; organizational personnel with information security and privacy responsibilities.

Interview: Organizational processes for implementing the insider threat program and the cross-discipline insider threat incident handling team; automated mechanisms supporting and/or implementing the insider threat program and the cross-discipline insider threat incident handling team.

PM-13: INFORMATION SECURITY AND PRIVACY WORKFORCE

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization establishes an information security workforce development and improvement program.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — The DFPS Commissioner or his/her designated representative(s) shall ensure that the agency has trained personnel to assist the agency in complying with the requirements of 1 TAC 202 and related policies. [Source: 1 TAC 202.20(4)]

Std.02 — The DFPS Information Security staff, with assistance from Human Resources and other internal and external partners, shall:

a. Ensure organizational information security workforce personnel obtain and continue to meet individual qualification standards, certification, and ongoing training for their assigned organization information security roles;

b. Annually re-evaluate the organization's workforce's knowledge and skill requirements based upon current risks and threats, and organization environment changes; and

c. Prioritize requirements for the development of training content to address the organization's information security workforce gaps and deficiencies.

SUPPLEMENTAL GUIDANCE

Information security workforce development and improvement programs include, for example: (i) defining the knowledge and skill levels needed to perform information security duties and tasks; (ii) developing role-based training programs for individuals assigned information security roles and responsibilities; and (iii) providing standards for measuring and building individual qualifications for incumbents and applicants for information security-related positions. Such workforce programs can also include associated information security career paths to encourage: (i) information security professionals to advance in the field and fill positions with greater responsibility; and (ii) organizations to fill information security-related positions with qualified personnel. Information security workforce development and improvement programs are complementary to organizational security awareness and training programs. Information security workforce development and improvement programs focus on developing and institutionalizing core information security capabilities of selected personnel needed to protect organizational operations, assets, and individuals.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** 1 TAC 202.20(4); DIR Security Control Standards Catalog **Federal**: OMB A-130; NIST SP 800-181.	AT-2, AT-3.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Information security program plan; privacy program plan; information security and privacy workforce development and improvement program documentation; procedures for the information security and privacy workforce development and improvement program; information security and privacy role-based training program documentation; other relevant documents or records

Interview: Organizational personnel with information security and privacy program planning and plan implementation responsibilities; organizational personnel responsible for the information security and privacy workforce development and improvement program; organizational personnel with information security and privacy responsibilities.

Test: Organizational processes for implementing the information security and privacy workforce development and improvement program; automated mechanisms supporting and/or implementing the information security and privacy workforce development and improvement program.

PM-14: TESTING, TRAINING, AND MONITORING

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization:

a. Implement a process for ensuring that organizational plans for conducting security and privacy testing, training, and monitoring activities associated with organizational systems:
   1. Are developed and maintained; and
   2. Continue to be executed; and

b. Review testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

A process for organization-wide security and privacy testing, training, and monitoring helps ensure that organizations provide oversight for testing, training, and monitoring activities and that those activities are coordinated. With the growing importance of continuous monitoring programs, the implementation of information security and privacy across the three levels of the risk management hierarchy and the widespread use of common controls, organizations coordinate and consolidate the testing and monitoring activities that are routinely conducted as part of ongoing assessments supporting a variety of controls.

Security and privacy training activities, while focused on individual systems and specific roles, require coordination across all organizational elements. Testing, training, and monitoring plans and activities are informed by current threat and vulnerability assessments.

REFERENCES	RELATED CONTROLS

Agency: DFPS Information Security Policy. **State:** 1 TAC 202.20(4); DIR Security Control Standards Catalog **Federal**: OMB A-130; NIST SP 800-37, 800-39, 800-53A, 800-115, 800-137.	AT-2, AT-3, CA-7, CP-4, IR-3, PM-12, SI-4.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Information security program plan; privacy program plan; plans for conducting security and privacy testing, training, and monitoring activities; organizational procedures addressing the development and maintenance of plans for conducting security and privacy testing, training, and monitoring activities; risk management strategy; procedures for the review of plans for conducting security and privacy testing, training, and monitoring activities for consistency with risk management strategy and risk response priorities; results of risk assessments associated with conducting security and privacy testing, training, and monitoring activities; documentation of the timely execution of plans for conducting security and privacy testing, training, and monitoring activities; other relevant documents or records.

Interview: Organizational personnel with responsibilities for developing and maintaining plans for conducting security and privacy testing, training, and monitoring activities; organizational personnel with information security and privacy responsibilities.

Test: Organizational processes for the development and maintenance of plans for conducting security and privacy testing, training, and monitoring activities; automated mechanisms supporting the development and maintenance of plans for conducting security and privacy testing, training, and monitoring activities.

PM-15: CONTACTS WITH SECURITY AND PRIVACY GROUPS AND ASSOCIATIONS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization establish and institutionalize contact with selected groups and associations within the security and privacy communities:

a. To facilitate ongoing security and privacy education and training for organizational personnel;

b. To maintain currency with recommended security and privacy practices, techniques, and technologies; and

c. To share current security and privacy information, including threats, vulnerabilities, and incidents.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Establish a process to receive, analyze and respond to reports of software vulnerabilities, including providing a means for external entities to contact the agency's security group. [Source: CIS 18.8 and CSF RS.AN-5]

Std.02 — Assemble and maintain information on third-party contact information to be used to report a security incident, such as law enforcement, relevant government departments, vendors, and Information Sharing and Analysis Center (ISAC) partners. [Source: CIS 19.5]

SUPPLEMENTAL GUIDANCE
Ongoing contact with security and privacy groups and associations is important in an environment of rapidly changing technologies and threats. Groups and associations include special interest groups, professional associations, forums, news groups, users' groups, and peer groups of security and privacy professionals in similar organizations. Organizations select security and privacy groups and associations based on mission and business functions. Organizations share threat, vulnerability, and incident information as well as contextual insights, compliance techniques, and privacy problems consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. Membership in organization-defined special interest groups or forums/services is considered as a means to: 1. Improve knowledge about best practices and staying up to date with relevant security information; 2. Ensure the understanding of the information security environment is current and complete (e.g., threat monitoring/intelligence services); 3. Receive early warnings of alerts, advisories, and patches pertaining to attacks and vulnerabilities; 4. Gain access to specialist information security advice; 5. Share and exchange information about new technologies, products, threats, or vulnerabilities; 6. Provide suitable liaison points when dealing with information security incidents. [Source: Hitrust CSF 05.g Contact with Special Interest Groups]

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog **Federal**: OMB A-130.	SA-11, SI-5.

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Information security program plan; privacy program plan; risk management strategy; procedures for establishing and institutionalizing contacts with security and privacy groups and associations; lists or other records of contacts with and/or membership in security and privacy groups and associations; other relevant documents or records. Interview: Organizational personnel with information security and privacy program planning and plan implementation responsibilities; organizational personnel responsible for establishing and institutionalizing contact with security and privacy groups and associations; organizational personnel with information security and privacy responsibilities; personnel from selected groups and associations with which the organization has established and institutionalized contact. Test: Organizational processes for establishing and institutionalizing contact with security and privacy groups and associations; automated mechanisms supporting contact with security and privacy groups and associations.

PM-16: THREAT AWARENESS PROGRAM	
Priority: P1	
Baseline(s): Low, Moderate, High	Overlay(s): DIR
CONTROL REQUIREMENTS	

The organization implements a threat awareness program that includes a cross-organization information-sharing capability.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Review environment of operation for indicators of compromise identified in threat intelligence alerts and advisories and take appropriate actions per incident response plan (see IR-04).

SUPPLEMENTAL GUIDANCE

Because of the constantly changing and increasing sophistication of adversaries, especially the advanced persistent threat (APT), it is becoming more likely that adversaries may successfully breach or compromise organizational information systems. One of the best techniques to address this concern is for organizations to share threat information. This can include, for example, sharing threat events (i.e., tactics, techniques, and procedures) that organizations have experienced, mitigations that organizations have found are effective against certain types of threats, threat intelligence (i.e., indications and warnings about threats that are likely to occur). Threat information sharing may be bilateral (e.g., government-commercial cooperatives, government-government cooperatives), or multilateral (e.g., organizations taking part in threat-sharing consortia). Threat information may be highly sensitive requiring special agreements and protection, or less sensitive and freely shared.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog **Federal**: OMB A-130.	SA-11, SI-5.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Information security program plan; privacy program plan; threat awareness program policy; threat awareness program procedures; risk assessment results relevant to threat awareness; documentation about the cross-organization information-sharing capability; other relevant documents or records.

Interview: Organizational personnel with information security and privacy program planning and plan implementation responsibilities; organizational personnel responsible for the threat awareness program; organizational personnel responsible for the cross-organization information-sharing capability; organizational personnel with information security and privacy responsibilities; external personnel with whom threat awareness information is shared by the organization.

Test: Organizational processes for implementing the threat awareness program; organizational processes for implementing the cross-organization information-sharing capability; automated mechanisms supporting and/or implementing the threat awareness program; automated mechanisms supporting and/or implementing the cross-organization information-sharing capability.

PM-16(01) AUTOMATED MEANS FOR SHARING THREAT INTELLIGENCE

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): Privacy

CONTROL REQUIREMENTS

The organization employs automated mechanisms to maximize the effectiveness of sharing threat intelligence information.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

To maximize the effectiveness of monitoring, it is important to know what threat observables and indicators the sensors need to be searching for. By using well-established frameworks, services, and automated tools, organizations improve their ability to rapidly share and feed the relevant threat detection signatures into monitoring tools.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** None. **Federal**: None.	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Information security program plan; privacy program plan; threat awareness program policy; threat awareness program procedures; risk assessment results related to threat awareness; documentation about the cross-organization information-sharing capability; other relevant documents or records.

Interview: Organizational personnel with information security and privacy program planning and plan implementation responsibilities; organizational personnel responsible for the threat awareness program; organizational personnel responsible for the cross-organization information-sharing capability; organizational personnel with information security and privacy responsibilities; external personnel with whom threat awareness information is shared by the organization,

Test: Organizational processes for implementing the threat awareness program; organizational processes for implementing the cross-organization information-sharing capability; automated mechanisms supporting and/or implementing the threat awareness program; automated mechanisms supporting and/or implementing the cross-organization information-sharing capability.

PM-18: PRIVACY PROGRAM PLAN

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization:

a. Develop and disseminate an organization-wide privacy program plan that provides an overview of the agency's privacy program, and:
   1. Includes a description of the structure of the privacy program and the resources dedicated to the privacy program;
   2. Provides an overview of the requirements for the privacy program and a description of the privacy program management controls and common controls in place or planned for meeting those requirements;
   3. Includes the role of the senior agency official for privacy and the identification and assignment of roles of other privacy officials and staff and their responsibilities;
   4. Describes management commitment, compliance, and the strategic goals and objectives of the privacy program;
   5. Reflects coordination among organizational entities responsible for the different aspects of privacy; and
   6. Is approved by a senior official with responsibility and accountability for the privacy risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; and

b. Update the plan biennially and to address changes in federal privacy laws and policy and organizational changes and problems identified during plan implementation or privacy control assessments.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

A privacy program plan is a formal document that provides an overview of an organization's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the senior agency official for privacy and other privacy officials and staff, the strategic goals and objectives of the privacy program, and the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks. Privacy program plans can be represented in single documents or compilations of documents.

The senior agency official for privacy is responsible for designating which privacy controls the organization will treat as program management, common, system-specific, and hybrid controls. Privacy program plans provide sufficient information about the privacy program management and common controls (including the specification of parameters and assignment and selection operations explicitly or by reference) to enable control implementations that are unambiguously compliant with the intent of the plans and a determination of the risk incurred if the plans are implemented as intended.

Program management controls are generally implemented at the organization level and are essential for managing the organization's privacy program. Program management controls are distinct from common, system-specific, and hybrid controls because program management controls are independent of any particular information system. Together, the privacy plans for individual systems and the organization-wide privacy program plan provide complete coverage for the privacy controls employed within the organization.

Common controls are documented in an appendix to the organization's privacy program plan unless the controls are included in a separate privacy plan for a system. The organization- wide privacy program plan indicates which separate privacy plans contain descriptions of privacy controls.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** TX Govt. Code 552.	PM-8, PM-9, PM-19.

Federal: Privacy Act; OMB A-130.	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Organizational personnel with privacy program planning and plan implementation responsibilities; organizational personnel with privacy responsibilities.

Interview: Organizational personnel with privacy program planning and plan implementation responsibilities; organizational personnel with privacy responsibilities.

PM-19: PRIVACY PROGRAM LEADERSHIP ROLE

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): Privacy

CONTROL REQUIREMENTS

The organization appoints a senior agency official for privacy with the authority, mission, accountability, and resources to coordinate, develop, and implement, applicable privacy requirements and manage privacy risks through the organization-wide privacy program.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — The DFPS Commissioner or his or her designated representative(s) shall designate a privacy officer to administer the state organization privacy program.

SUPPLEMENTAL GUIDANCE

The privacy officer is an organizational official. For federal agencies—as defined by applicable laws, executive orders, directives, regulations, policies, standards, and guidelines—this official is designated as the senior agency official for privacy. Organizations may also refer to this official as the chief privacy officer.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** None. **Federal**: Privacy Act; OMB A-130.	PM-18, PM-20, PM-23, PM-24, PM-27.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Privacy program documents, including policies, procedures, plans, and reports; public privacy notices, including Federal Register notices; privacy impact assessments; privacy risk assessments; Privacy Act statements; system of records notices; computer matching agreements and notices; contracts, information sharing agreements, and memoranda of understanding; governing requirements, including laws, Executive Orders, regulations, standards, and guidance; other relevant documents or records.

Interview: Organizational personnel with privacy program planning and plan implementation responsibilities; organizational personnel with privacy responsibilities; senior agency official for privacy; privacy officials.

PM-20: DISSEMINATION OF PRIVACY PROGRAM INFORMATION

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): Privacy

CONTROL REQUIREMENTS

The organization maintains a central resource webpage on the organization's principal public website that serves as a central source of information about the organization's privacy program and that:

a. Ensures that the public has access to information about organizational privacy activities and can communicate with its senior agency official for privacy;

b. Ensures that organizational privacy practices and reports are publicly available; and

c. Employs publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Include contact information and a link to the Privacy Notice or Privacy Policy on all public-facing agency websites.

Std.02 — Post the agency Privacy Notice to a publicly accessible website.

SUPPLEMENTAL GUIDANCE

For federal agencies, the webpage is located at www.[agency].gov/privacy. Federal agencies include public privacy impact assessments, system of records notices, computer matching notices and agreements, Privacy Act exemption and implementation rules, privacy reports, privacy policies, instructions for individuals making an access or amendment request, email addresses for questions/complaints, blogs, and periodic publications.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** Texas Cybersecurity Framework. **Federal**: Privacy Act; OMB A-130; M-17-06.	AC-3, PM-19, PT-5, PT-6, PT-7, RA-8.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Public website; publicly posted privacy program documents, including policies, procedures, plans, and reports; position description of the senior agency official for privacy; public privacy notices, including Federal Register notices; privacy impact assessments; privacy risk assessments; Privacy Act statements and system of records notices; computer matching agreements and notices; other relevant documents or records

Interview: Organizational personnel with privacy program information dissemination responsibilities; organizational personnel with privacy responsibilities.

Test: Location, access, availability, and functionality of privacy resource webpage

PM-20(01): PRIVACY POLICIES ON WEBSITES, APPLICATIONS, AND DIGITAL SERVICES

Priority: P1

Baseline(s): N/A	Overlay(s): Privacy

CONTROL REQUIREMENTS

The organization develop and post privacy policies on all external-facing websites, mobile applications, and other digital services, that:

a. Are written in plain language and organized in a way that is easy to understand and navigate;

b. Provide information needed by the public to make an informed decision about whether and how to interact with the organization; and

c. Are updated whenever the organization makes a substantive change to the practices it describes and includes a time/date stamp to inform the public of the date of the most recent changes.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS shall prominently post a link to the policy statement on a generally accessible Internet site maintained by or for the agency. [Source: TX Govt. Code 2054.126(b)]

Std.02 — DFPS posted privacy policy shall include statements:

a. Generally allowing the use and reproduction of information on a state agency's Internet site without the state agency's permission, subject to specified conditions;

b. Generally allowing linking from a web page to a page on a state agency's Internet site without the state agency's permission, subject to specified conditions;

c. Prohibiting a state agency from charging a fee to access, use, reproduce information on, or link to its Internet site except to the extent the state agency is specifically authorized to do so by the legislature;

d. Requiring that the state agency's Internet site be credited as the source of information reproduced from the site and requiring that the date that the material was reproduced from the site be clearly stated;

e. Prohibiting a state agency from selling or releasing an e-mail address of a member of the public unless the member of the public affirmatively consents to the sale or release of the e- mail address; and

f. Specifying other policies necessary to protect from public disclosure personal information submitted by a member of the public to a state agency's Internet site to the extent the information is:

    1. Confidential;
    2. Excepted from the requirements of Section 552.021; or
    3. Protected by other law intended to protect a person's privacy interests. [Source: TX Govt. Code 2054.126(c)]

Std.03 — Ensure that a link to the Privacy & Security Policy is included on all publicly accessible agency websites.

Std.04 — Review and formally approve the Privacy & Security Policy at least once every three years.

SUPPLEMENTAL GUIDANCE

Organizations post privacy policies on all external-facing websites, mobile applications, and other digital services. Organizations post a link to the relevant privacy policy on any known, major entry points to the website, application, or digital service. In addition, organizations provide a link to the privacy policy on any webpage that collects personally identifiable information. Organizations may be subject to applicable laws, executive orders, directives, regulations, or policies that require the provision of specific information to the public.

Organizational personnel consult with the senior agency official for privacy and legal counsel regarding such requirements.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** Texas Cybersecurity Framework. **Federal**: Privacy Act; OMB A-130; M-17-06.	AC-3, PM-19, PT-5, PT-6, PT-7, RA-8.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Public website; publicly posted privacy program documents, including policies, procedures, plans, and reports; position description of the senior agency official for privacy; public privacy notices, including Federal Register notices; privacy impact assessments; privacy risk assessments; Privacy Act statements and system of records notices; computer matching agreements and notices; other relevant documents or records

Interview: Organizational personnel with privacy program information dissemination responsibilities; organizational personnel with privacy responsibilities.

Test: Location, access, availability, and functionality of privacy resource webpage.

PM-21: ACCOUNTING OF DISCLOSURES

Priority: P1

Baseline(s): N/A	Overlay(s): Privacy

CONTROL REQUIREMENTS

The organization:

a. Develop and maintain an accurate accounting of disclosures of personally identifiable information, including:
   1. Date, nature, and purpose of each disclosure; and
   2. Name and address, or other contact information of the individual or organization to which the disclosure was made;
b. Retain the accounting of disclosures for the length of the time the personally identifiable information is maintained or five years after the disclosure is made, whichever is longer; and
c. Make the accounting of disclosures available to the individual to whom the personally identifiable information relates upon request.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

The purpose of accounting of disclosures is to allow individuals to learn to whom their personally identifiable information has been disclosed, to provide a basis for subsequently advising recipients of any corrected or disputed personally identifiable information, and to provide an audit trail for subsequent reviews of organizational compliance with conditions for disclosures. For federal agencies, keeping an accounting of disclosures is required by the Privacy Act; agencies should consult with their senior agency official for privacy and legal counsel on this requirement and be aware of the statutory exceptions and OMB guidance relating to the provision.

Organizations can use any system for keeping notations of disclosures, if it can construct from such a system, a document listing of all disclosures along with the required information. Automated mechanisms can be used by organizations to determine when personally identifiable information is disclosed, including commercial services that provide notifications and alerts. Accounting of disclosures may also be used to help organizations verify compliance with applicable privacy statutes and policies governing the disclosure or dissemination of information and dissemination restrictions.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; Breaches of Confidential Records or Sensitive Personal Information. **State:** TX Govt. Code 552. **Federal**: Privacy Act; OMB A-130.	AC-3, AU-2, PT-2.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Privacy program plan; disclosure policies and procedures; records of disclosures; audit logs; Privacy Act policies and procedures; system of records notice; Privacy Act exemption rules.

Interview: Organizational personnel with privacy program responsibilities; organizational personnel with privacy responsibilities.

Test: Organizational processes for disclosures; automated mechanisms supporting the accounting of disclosures, including commercial services that provide notifications and alerts.

PM-25: MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION USED IN TESTING, TRAINING, AND RESEARCH

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): Privacy

CONTROL REQUIREMENTS

The organization:

a. Develop, document, and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research;

b. Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes;

c. Authorize the use of personally identifiable information when such information is required for internal testing, training, and research; and

d. Review and update policies and procedures at the frequencies specified in Std.02.

e.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Ensure that test plan documentation includes rationale for use of sensitive personal information (SPI), risk minimization techniques, and removal of SPI at the conclusion of tests.

Std.02 — Review, and update as required:

a. Policies every three years; and

b. Procedures annually.

SUPPLEMENTAL GUIDANCE

The use of personally identifiable information in testing, research, and training increases the risk of unauthorized disclosure or misuse of such information. Organizations consult with the senior agency official for privacy and/or legal counsel to ensure that the use of personally identifiable information in testing, training, and research is compatible with the original purpose for which it was collected. When possible, organizations use placeholder data to avoid exposure of personally identifiable information when conducting testing, training, and research.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** None. **Federal**: Privacy Act; OMB A-130.	PM-23, PT-3, SA-3, SA-8, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Privacy program plan; policies and procedures for the minimization of personally identifiable information used in testing, training, and research; documentation supporting policy implementation (e.g., templates for testing, training, and research; privacy threshold analysis; privacy risk assessment); data sets used for testing, training, and research

Interview: Organizational personnel with privacy program responsibilities; organizational personnel with privacy responsibilities; system developers; personnel with IRB responsibilities.

Test: Organizational processes for data quality and personally identifiable information management; automated mechanisms supporting data quality management and personally identifiable information management to minimize the use of personally identifiable information.

PM-26: COMPLAINT MANAGEMENT

Priority: P1	
Baseline(s): Low, Moderate, High	Overlay(s): Privacy

CONTROL REQUIREMENTS

The organization implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational security and privacy practices that includes:

a. Mechanisms that are easy to use and readily accessible by the public;

b. All information necessary for successfully filing complaints;

c. Tracking mechanisms to ensure all complaints received are reviewed and addressed within 60 days;

d. Acknowledgement of receipt of complaints, concerns, or questions from individuals within a time period not to exceed five business days; and

e. Response to complaints, concerns, or questions from individuals within a time period not to exceed 10 days.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Designate one mailing address and one e-mail address for receiving complaints, concerns, and questions from individuals about privacy practices. Ensure that information is posted on public websites and physical signs to be placed in areas of facilities open to the public.

SUPPLEMENTAL GUIDANCE

Complaints, concerns, and questions from individuals can serve as valuable sources of input to organizations and ultimately improve operational models, uses of technology, data collection practices, and controls. Mechanisms that can be used by the public include telephone hotline, email, or web-based forms. The information necessary for successfully filing complaints includes contact information for the senior agency official for privacy or other official designated to receive complaints. Privacy complaints may also include personally identifiable information which is handled in accordance with relevant policies and processes.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** TX Govt. Code 552. **Federal**: Privacy Act; OMB A-130.	IR-7, IR-9, PM-22, SI-18.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Privacy program plan; procedures addressing complaint management; complaint documentation; procedures addressing the reviews of complaints; other relevant documents or records

Interview: Organizational personnel with privacy program responsibilities; organizational personnel with privacy responsibilities.

Test: Organizational processes for complaint management; automated mechanisms supporting complaint management; tools used by the public to submit complaints, concerns, and questions (e.g., telephone, hotline, email, or web-based forms.

PM-27: PRIVACY REPORTING

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): Privacy

CONTROL REQUIREMENTS

The organization:

a. Develop privacy reports as defined in state legislation and the privacy policy and disseminate to:
   1. Oversight bodies as specified in state legislation and the privacy policy to demonstrate accountability with statutory, regulatory, and policy privacy mandates; and
   2. Officials as defined in the privacy policy and other personnel with responsibility for monitoring privacy program compliance; and

b. Review and update privacy reports at least biennially.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Through internal and external reporting, organizations promote accountability and transparency in organizational privacy operations. Reporting can also help organizations to determine progress in meeting privacy compliance requirements and privacy controls, compare performance across the federal government, discover vulnerabilities, identify gaps in policy and implementation, and identify models for success. For federal agencies, privacy reports include annual senior agency official for privacy reports to OMB, reports to Congress required by Implementing Regulations of the 9/11 Commission Act, and other public reports required by law, regulation, or policy, including internal policies of organizations. The senior agency official for privacy consults with legal counsel, where appropriate, to ensure that organizations meet all applicable privacy reporting requirements.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** TX Govt. Code 552. **Federal**: FISMA; OMB A-108, A-130.	IR-9, PM-19.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Privacy program plan; internal and external privacy reports; privacy program plan; annual senior agency official for privacy reports to OMB; reports to Congress required by law, regulation, or policy, including internal policies; records documenting the dissemination of reports to oversight bodies and officials responsible for monitoring privacy program compliance; records of review and updates of privacy reports.

Interview: Organizational personnel with privacy program responsibilities; organizational personnel with privacy responsibilities; legal counsel

PM-28: RISK FRAMING

Priority: P1	
Baseline(s): Low, Moderate, High	Overlay(s): Privacy

CONTROL REQUIREMENTS

The organization:

a. Identify and document:
   1. Assumptions affecting risk assessments, risk responses, and risk monitoring;
   2. Constraints affecting risk assessments, risk responses, and risk monitoring;
   3. Priorities and trade-offs considered by the organization for managing risk; and
   4. Organizational risk tolerance;

b. Distribute the results of risk framing activities to personnel as identified in the Information Security and Privacy policy; and

c. Review and update risk framing considerations annually.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Require that senior leaders/executives, in consultation and collaboration with the risk executive (function), define the organizational risk frame including the types of risk decisions (e.g., risk responses) supported, how and under what conditions risk is assessed to support those risk decisions, and how risk is monitored (e.g., to what level of detail, in what form, and with what frequency). [Source: SP 800-39]

Std.02 — Document the results of risk framing exercises in accordance to the DFPS Information Risk Management Policy.

SUPPLEMENTAL GUIDANCE

Risk framing is most effective when conducted at the organization level and in consultation with stakeholders throughout the organization including mission, business, and system owners. The assumptions, constraints, risk tolerance, priorities, and trade-offs identified as part of the risk framing process inform the risk management strategy, which in turn informs the conduct of risk assessment, risk response, and risk monitoring activities. Risk framing results are shared with organizational personnel, including mission and business owners, information owners or stewards, system owners, authorizing officials, senior agency information security officer, senior agency official for privacy, and senior accountable official for risk management.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Information Risk Management Policy. **State:** None. **Federal**: OMB A-130; NIST SP 800-39	CA-7, PM-9, RA-3, RA-7.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Information security program plan; privacy program plan; supply chain risk management strategy; documentation of risk framing activities; policies and procedures for risk framing activities; risk management strategy.

Interview: Organizational personnel (including mission, business, and system owners or stewards; authorizing officials; senior agency information security officer; senior agency official for privacy; and senior accountable official for risk management).

Test: Organizational procedures and practices for authorizing, conducting, managing, and reviewing personally identifiable information processing; organizational processes for risk framing; automated mechanisms supporting the development, review, update, and approval of risk framing.

PM-30: SUPPLY CHAIN RISK MANAGEMENT STRATEGY

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization:

a. Develop an organization-wide strategy for managing supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services;

b. Implement the supply chain risk management strategy consistently across the organization; and

c. Review and update the supply chain risk management strategy on an annual basis or as required, to address organizational changes.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — The DFPS supply chain risk management strategy must align with NIST's Risk Management Framework and includes the DFPS Information Security and Privacy Controls Standards Catalog.

SUPPLEMENTAL GUIDANCE

An organization-wide supply chain risk management strategy includes an unambiguous expression of the supply chain risk appetite and tolerance for the organization, acceptable supply chain risk mitigation strategies or controls, a process for consistently evaluating and monitoring supply chain risk, approaches for implementing and communicating the supply chain risk management strategy, and the associated roles and responsibilities. Supply chain risk management includes considerations of the security and privacy risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services. The supply chain risk management strategy can be incorporated into the organization's overarching risk management strategy and can guide and inform supply chain policies and system-level supply chain risk management plans. In addition, the use of a risk executive function can facilitate a consistent, organization-wide application of the supply chain risk management strategy. The supply chain risk management strategy is implemented at the organization and mission/business levels, whereas the supply chain risk management plan (see SR-02) is implemented at the system level.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Information Risk Management Policy. **State:** None. **Federal**: Privacy Act; Secure Technology Act; 41 CFR 201; EO 13873; OMB A-130, M-17-06; ISO 27036, I20243; NIST SP 800-161; NIST IR 8272; CNSSD 505.	CM-10, PM-9, SR-1, SR-2, SR-3, SR-4, SR-5, SR-6, SR-7, SR-8, SR-9, SR-11.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Supply chain risk management strategy; organizational risk management strategy; enterprise risk management documents; other relevant documents or records.

Interview: Organizational personnel with supply chain risk management responsibilities; organizational personnel with information security responsibilities; organizational personnel with acquisition responsibilities; organizational personnel with enterprise risk management responsibilities.

PM-31: CONTINUOUS MONITORING STRATEGY

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): Privacy

CONTROL REQUIREMENTS

The organization develop an organization-wide continuous monitoring strategy and implement continuous monitoring programs that includes:

a. Establishing the following organization-wide metrics to be monitored: metrics defined in the Continuous Monitoring Program;

b. Establishing frequencies as specified in the Continuous Monitoring Program for monitoring and frequencies as specified in the risk management program policy for assessment of control effectiveness;

c. Ongoing monitoring of organizationally defined metrics in accordance with the continuous monitoring strategy;

d. Correlation and analysis of information generated by control assessments and monitoring;

e. Response actions to address results of the analysis of control assessment and monitoring information; and

f. Reporting the security and privacy status of organizational systems to personnel or roles as defined in Stds.02 & 03 at the frequency defined in Stds.02 & 03.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — The DFPS Continuous Monitoring Program must align with NIST's Risk Management Framework and includes the DFPS Information Security and Privacy Controls Catalog.

Std.02 — The DFPS Chief Information Security Officer shall be responsible for reporting, at least annually, to the DFPS Commissioner the status and effectiveness of security controls. [Source: 1 TAC 202.21(b)(11)]

Std.03 — The DFPS Chief Information Security Officer shall report, at least annually, to the DFPS Commissioner on the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the requirements of 1 TAC 202 and the effectiveness of current information security program and status of key initiatives. [Source: 1 TAC 202.23(a), (a)(1)]

SUPPLEMENTAL GUIDANCE

Continuous monitoring at the organization level facilitates ongoing awareness of the security and privacy posture across the organization to support organizational risk management decisions. The terms "continuous" and

"ongoing" imply that organizations assess and monitor their controls and risks at a frequency sufficient to support risk-based decisions.

Different types of controls may require different monitoring frequencies. The results of continuous monitoring guide and inform risk response actions by organizations. Continuous monitoring programs allow organizations to maintain the authorizations of systems and common controls in highly dynamic environments of operation with changing mission and business needs, threats, vulnerabilities, and technologies. Having access to security- and privacy-related information on a continuing basis through reports and dashboards gives organizational officials the capability to make effective, timely, and informed risk management decisions, including ongoing authorization decisions. To further facilitate security and privacy risk management, organizations consider aligning organization-defined monitoring metrics with organizational risk tolerance as defined in the risk management strategy. Monitoring requirements, including the need for monitoring, may be referenced in other controls and control enhancements such as, AC-02g, AC-17(01), AT-04a, CA-07, CM- 03f, CM-06d, CM-11c, IR-05, MA-02b, MA-03a, MA-04a, PE-03d, PE-06, PE-14b, PE-16, PM- 06, PS-07e, SA-09c, SC-07a, SC-07(24)b, SC-18b, SI-04.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** 1 TAC 202.21(b)(11), 1 TAC 202.23(a), (a)(1). **Federal**: NIST SP 800-37, 800-39, 800-137, 800-137A.	AC-2, AC-6, AC-17, AT-4, AU-6, AU-13, CA-2, CA-5, CA-6, CA-7, CM-3, CM-4, CM-6, CM-11, IA-5, IR-5, MA-2, MA-3, MA-4, PE-3, PE-6, PE-14, PE-16, PE-20, PL-2, PM-4, PM-6, PM-9, PM-10, PM-12, PM-14, PM-23, PM-28, PS-7, PT-7, RA-3, RA-5, RA-7, SA-9, SA-11, SC-5, SC-7, SC-18, SC-38, SC-43, SI-3, SI-4, SI-12, SR-2, SR-4.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Information security program plan; privacy program plan; supply chain risk management plan; continuous monitoring strategy; risk management strategy; information security continuous monitoring program documentation, reporting, metrics, and artifacts; information security continuous monitoring program assessment documentation, reporting, metrics, and artifacts; assessment and authorization policy; procedures addressing the continuous monitoring of controls; privacy program continuous monitoring documentation, reporting, metrics, and artifacts; continuous monitoring program records, security, and privacy impact analyses; status reports; risk response documentation; other relevant documents or records.

Interview: Senior Accountable Official for Risk Management; chief information officer; senior agency information security officer; senior agency official for privacy; organizational personnel with information security, privacy, and supply chain risk management program responsibilities.

Test: Organizational procedures and mechanisms used for information security, privacy, and supply chain continuous monitoring.

PM-32: PURPOSING

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization analyzes all systems or system components under configuration management supporting mission essential services or functions to ensure that the information resources are being used consistent with their intended purpose

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Review system security plans (SSPs) to ensure that all systems and system components have sufficient capacity and are appropriately protected based on risk.

SUPPLEMENTAL GUIDANCE

Initial authorization to operate is based on evidence available at one point in time, but systems and environments of operation change. Ongoing assessment of security control effectiveness supports a system's security authorization over time in highly dynamic environments of operation with changing threats, vulnerabilities, technologies, and missions/business processes. Through Information Security Continuous Monitoring (ISCM), new threat or vulnerability information is evaluated as it becomes available, permitting organizations to make adjustments to security requirements or individual controls as needed to maintain authorization decisions. [Source: SP 800-137 2.2 Ongoing System Authorizations]

Systems are designed to support a specific mission or business function. However, over time, systems and system components may be used to support services and functions that are outside of the scope of the intended mission or business functions. This can result in exposing information resources to unintended environments and uses that can significantly increase threat exposure. In doing so, the systems are more vulnerable to compromise, which can ultimately impact the services and functions for which they were intended. This is especially impactful for mission-essential services and functions. By analyzing resource use, organizations can identify such potential exposures.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** None. **Federal**: NIST SP 800-160-1, 800-160-2.	CA-7, PL-2, RA-3, RA-9.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Information security program plan; privacy program plan; list of essential services and functions; organizational analysis of information resources; risk management strategy; other relevant documents or records.

Interview: Organizational personnel with information security, privacy, and supply chain risk management program responsibilities.

(PS) PERSONNEL SECURITY

Personnel Security are standards around personnel screening, termination, transfers, sanctions, and access agreements are all examples of PS controls to protect employees.

DFPS human resources policies and procedures are established to ensure that individuals occupying positions of responsibility within DFPS, including third-party service providers, are trustworthy and meet established security criteria for those positions. Personnel security ensures that DFPS

information and information systems are protected during and after personnel actions such as terminations and transfers. DFPS employs formal sanctions for personnel failing to comply with DFPS security policies and procedures.

PS-01: PERSONNEL SECURITY POLICY AND PROCEDURES	
Priority: P1	
Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Develop, document, and disseminate to appropriate personnel:
   1. Organization-level personnel security policy that:
      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls;

b. Designate a senior management official as defined in the personnel security policy to manage the development, documentation, and dissemination of the personnel security policy and procedures; and

c. Review and update the current personnel security:
   1. Policy every two (2) years and following major changes to legislation or security requirements; and
   2. Procedures every two (2) years and following major changes to legislation or security requirements.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS must have a formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. [Source: DIR Control Standards Catalog PS-1]

Std.02 — The DFPS Chief Information Security Officer shall be responsible for:

a. Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks;

b. Providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities under 1 TAC 202; and

c. Developing and recommending policies and establishing procedures and practices, in cooperation with the agency Information Resources Manager, information-owners and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, or disclosure. [Source: 1 TAC 202.21(b)(3, 5, 8)]

SUPPLEMENTAL GUIDANCE

Personnel security policy and procedures for the controls in the PS family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on their development. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission level or system-specific policies and procedures. The policy can be included as part of the general security and privacy

policy or be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs, for mission/business processes, and for systems, if needed.

Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to personnel security policy and procedures include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Information Security Program Policy. **State:** DIR Security Control Standards Catalog. **Federal**: NIST SP 800-12, 800-30, 800-39, 800-100; FBI CJIS CSP v5.9	PM-9, PS-8, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy and procedures; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with access control responsibilities; organizational personnel with information security with information security and privacy responsibilities.

PS-02: POSITION RISK DESIGNATION

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Assign a risk designation to all organizational positions;

b. Establish screening criteria for individuals filling those positions; and

c. Review and update position risk designations annually, when the position is updated, and when the position is vacated.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — All authorized users (including, but not limited to, state organization personnel, temporary employees, and employees of independent contractors) of the state organization's information resources, shall formally acknowledge that they will comply with the security policies and procedures of the state organization or they shall not be granted access to information resources. The state organization head or his or her designated representative will determine the method of acknowledgement and how often this acknowledgement must be re-executed by the user to maintain access to state organization information resources. [Source: DIR Control Standards Catalog PS-2]

SUPPLEMENTAL GUIDANCE

Position risk designations reflect Office of Personnel Management (OPM) policy and guidance. Proper position designation is the foundation of an effective and consistent suitability and personnel security program. The Position Designation System (PDS) assesses the duties and responsibilities of a position to determine the degree of potential damage to the efficiency or integrity of the service due to misconduct of an incumbent of a position and establishes the risk level of that position. The PDS assessment also determines if the duties and responsibilities of the position present the potential for position incumbents to bring about a material adverse effect on national security and the degree of that potential effect, which establishes the sensitivity level of a position. The results of the assessment determine what level of investigation is conducted for a position. Risk designations can guide and inform the types of authorizations that individuals receive when accessing organizational information and information systems. Position screening criteria include explicit information security role appointment requirements. Parts 1400 and 731 of Title 5, Code of Federal Regulations, establish the requirements for organizations to evaluate relevant covered positions for a position sensitivity and position risk designation commensurate with the duties and responsibilities of those positions.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Information Security Program Policy. **State:** DIR Security Control Standards Catalog. **Federal**: 5 CFR 731; NIST SP 800-181; FBI CJIS CSP v5.9	AC-5, AT-3, PE-2, PE-3, PL-2, PS-3, PS-6, SA-5, SA-21, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; personnel termination policy and procedure; personnel transfer policy and procedure; procedures for addressing account management; system design documentation; system configuration settings and associated documentation; list of active system accounts along with the name of the individual associated with each account; list of recently disabled system accounts and the name of the individual associated with each account; list of conditions for group and role membership; notifications of recent transfers, separations, or terminations of employees; access authorization records; account management compliance reviews; system monitoring records; system audit records; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security with information security and privacy responsibilities.

Test: Organizational processes for account management on the system; automated mechanisms for implementing account management.

PS-03: PERSONNEL SCREENING

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Screen individuals prior to authorizing access to the system; and

b. Rescreen individuals in accordance with rescreening conditions defined in Human Resources policies and procedures, and, where rescreening is indicated, before access is granted for any new or changed role.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS must screen individuals requiring access to organizational information and information systems before authorizing access. [Source: DIR Control Standards Catalog PS- 3]

SUPPLEMENTAL GUIDANCE

Position risk designations reflect Office of Personnel Management (OPM) policy and guidance. Proper position designation is the foundation of an effective and consistent suitability and personnel security program. The Position Designation System (PDS) assesses the duties and responsibilities of a position to determine the degree of potential damage to the efficiency or integrity of the service due to misconduct of an incumbent of a position and establishes the risk level of that position. The PDS assessment also determines if the duties and responsibilities of the position present the potential for position incumbents to bring about a material adverse effect on national security and the degree of that potential effect, which establishes the sensitivity level of a position. The results of the assessment determine what level of investigation is conducted for a position. Risk designations can guide and inform the types of authorizations that individuals receive when accessing organizational information and information systems. Position screening criteria include explicit information security role appointment requirements. Parts 1400 and 731 of Title 5, Code of Federal Regulations, establish the requirements for organizations to evaluate relevant covered positions for a position sensitivity and position risk designation commensurate with the duties and responsibilities of those positions.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Information Security Program Policy. **State:** DIR Security Control Standards Catalog. **Federal**: EO 13526, 13587; FIPS 199, 201; NIST SP 800-60-1, 800-60-2, 800-73-4, 800-76-2, 800-78-4; PCI DSS; FBI CJIS CSP v5.9	AC-2, IA-4, MA-5, PE-2, PM-12, PS-2, PS-6, PS-7, SA-21.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing access enforcement; system design documentation; system configuration settings and associated documentation; list of approved authorizations (user privileges); system audit records; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with access enforcement responsibilities; system/network administrators; organizational personnel with information security and privacy responsibilities; system developers.

Test: Automated mechanisms implementing access control policy.

PS-04: PERSONNEL TERMINATION

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization, upon termination of individual employment:

a. Disable system access within one working day for voluntary terminations, and as soon as possible, but no later than eight hours of any involuntary termination;

b. Terminate or revoke any authenticators and credentials associated with the individual;

c. Conduct exit interviews that include a discussion of all security constraints and continued obligations under non-disclosure, confidentiality, user access agreements, and applicable regulations;

d. Retrieve all security-related organizational system-related property; and

e. Retain access to organizational information and systems formerly controlled by the terminated individual.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS, upon termination of individual employment, must terminate information system access, retrieve all organizational information system-related property, and provide appropriate personnel with access to official records created by the terminated employee that are stored on organizational information systems. [Source: DIR Control Standards Catalog PS-4]

SUPPLEMENTAL GUIDANCE

System property includes hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for system-related property. Security topics at exit interviews include reminding individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not always be possible for some individuals, including in cases related to the unavailability of supervisors, illnesses, or job abandonment. Exit interviews are important for individuals with security clearances. The timely execution of termination actions is essential for individuals who have been terminated for cause. In certain situations, organizations consider disabling the system accounts of individuals who are being terminated prior to the individuals being notified.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Information Security Program Policy. **State:** DIR Security Control Standards Catalog. **Federal**: EO 13526, 13587; FIPS 199, 201; NIST SP 800-60-1, 800-60-2, 800-73-4, 800-76-2, 800-78-4; PCI DSS; FBI CJIS CSP v5.9	AC-2, IA-4, PE-2, PM-12, PS-6, PS-7.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Personnel security policy; procedures addressing personnel termination; records of personnel termination actions; list of system accounts; records of terminated or revoked authenticators/credentials; records of exit interviews; system security plan; other relevant documents or records.

Interview: Organizational personnel with personnel security responsibilities; organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities.

Test: Organizational processes for personnel termination; automated mechanisms supporting and/or implementing personnel termination notifications; automated mechanisms for disabling system access/revoking authenticators.

PS-05: PERSONNEL TRANSFER

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the organization;

b. Initiate reassignment actions to ensure all system access no longer required is removed or disabled within 24 hours following the formal transfer action;

c. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and

d. Notify personnel identified in System Security Plans (SSPs) within 24 hours if not otherwise defined in policy.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Review information systems/facilities access authorizations when personnel are reassigned or transferred to other positions within the organization and initiate appropriate actions. [Source: DIR Control Standards Catalog PS-5]

Std.02 — Require re-authorization for privileged access, to ensure such access is only granted where appropriate for the new role and responsibilities.

Std.03 — Ensure facility access codes, if used, are modified to prevent misuse by personnel no longer require access.

Std.04 — Collect system-related property no longer required for personnel in new positions.

SUPPLEMENTAL GUIDANCE

Personnel transfer applies when reassignments or transfers of individuals are permanent or of such extended duration as to make the actions warranted. Organizations define actions appropriate for the types of reassignments or transfers, whether permanent or extended.

Actions that may be required for personnel transfers or reassignments to other positions within organizations include returning old and issuing new keys, identification cards, and building passes; closing system accounts and establishing new accounts; changing system access authorizations (i.e., privileges); and providing for access to official records to which individuals had access at previous work locations and in previous system accounts.

REFERENCES	RELATED CONTROLS

Agency: DFPS Information Security Policy; DFPS Information Security Program Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FBI CJIS CSP v5.9	AC-2, IA-4, PE-2, PM-12, PS-4, PS-7.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Personnel security policy; procedures addressing personnel transfer; records of personnel transfer actions; list of system and facility access authorizations; system security plan; other relevant documents or records.

Interview: Organizational personnel with personnel security responsibilities; organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities.

Test: Organizational processes for personnel transfer; automated mechanisms supporting and/or implementing personnel transfer notifications; automated mechanisms for disabling system access/revoking authenticators.

PS-06: ACCESS AGREEMENTS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Develop and document access agreements for organizational systems;
b. Review and update the access agreements bi-annually; and
c. Verify that individuals requiring access to organizational information and systems:
    1. Sign appropriate access agreements prior to being granted access; and
    2. Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or at least bi-annually.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Complete appropriate signed access agreements for individuals requiring access to organizational information and information systems before authorizing access. [Source: DIR Control Standards Catalog PS-6]

Std.02 — Develop a data use agreement (DUA)/Acceptable Use Agreement/Memorandum of Understanding (MOU) for use by the agency that meets the particular needs of the agency and is consistent with rules adopted by the Department of Information Resources that relate to information security standards for state agencies.

SUPPLEMENTAL GUIDANCE

Access agreements include nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with organizational systems to which access is authorized.

Organizations can use electronic signatures to acknowledge access agreements unless specifically prohibited by organizational policy.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Information Security Program Policy. **State:** TX Govt. Code 2054.134, TX Govt. Code 2054.135; DIR Security Control Standards Catalog. **Federal**: FBI CJIS CSP v5.9	AC-17, PE-2, PL-4, PS-2, PS-3, PS-6, PS-7, PS-8, SA-21, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Personnel security policy; personnel security procedures; procedures addressing access agreements for organizational information and systems; access control policy; access control procedures; access agreements (including non-disclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements); documentation of access agreement reviews, updates, and re-signing; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with personnel security responsibilities; organizational personnel who have signed/resigned access agreements; organizational personnel with information security and privacy responsibilities.

Test: Organizational processes for reviewing, updating, and re-signing access agreements; automated mechanisms supporting the reviewing, updating, and re-signing of access agreements.

PS-06(02): CLASSIFIED INFORMATION REQUIRING SPECIAL PROTECTION

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization ensures that access to classified information requiring special protection is granted only to individuals who:

a. Have a valid access authorization that is demonstrated by assigned official government duties;

b. Satisfy associated personnel security criteria; and

c. Have read, understood, and signed a nondisclosure agreement.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Complete appropriate signed access agreements for individuals requiring access to FBI CJIS information and information systems before authorizing access.

SUPPLEMENTAL GUIDANCE
Classified information requiring special protection includes, for example, collateral information, Special Access Program (SAP) information, and Sensitive Compartmented Information (SCI). Personnel security criteria reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Information Security Program Policy; DPS Security and Management Control Outsourcing Standard for Non-Channelers. **State:** None. **Federal**: FBI CJIS CSP v5.9	AC-17, PE-2, PL-4, PS-2, PS-3, PS-6, PS-7, PS-8, SA-21, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Personnel security policy; procedures addressing access agreements for organizational information and systems; access agreements; access authorizations; personnel security criteria; signed non-disclosure agreements; system security plan; other relevant documents or records.

Interview: Organizational personnel with personnel security responsibilities; organizational personnel who have signed non-disclosure agreements; organizational personnel with information security responsibilities.

Test: Organizational processes for access to classified information requiring special protection.

PS-07: THIRD-PARTY PERSONNEL SECURITY

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Establish personnel security requirements, including security roles and responsibilities for external providers;

b. Require external providers to comply with personnel security policies and procedures established by the organization;

c. Document personnel security requirements;

d. Require external providers to notify personnel as identified in contracts or System Security Plans (SSPs) of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within 24 hours; and

e. Monitor provider compliance with personnel security

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Establish personnel security requirements including security roles and responsibilities for third-party providers and monitor provider compliance. [Source: DIR Control Standards Catalog PS-7]

Std.02 — Ensure that contractors receive appropriate security and privacy awareness training and agree to comply with organizational policies (see AT-02).

Std.03 — Include personnel security requirements, including screening, training, and compliance, in contract language.

SUPPLEMENTAL GUIDANCE

External provider refers to organizations other than the organization operating or acquiring the system. External providers include service bureaus, contractors, and other organizations that provide system development, information technology services, testing or assessment services, outsourced applications, and network/security management. Organizations explicitly include personnel security requirements in acquisition-related documents. External providers may have personnel working at organizational facilities with credentials, badges, or system privileges issued by organizations. Notifications of external personnel changes ensure the appropriate termination of privileges and credentials. Organizations define the transfers and terminations deemed reportable by security-related characteristics that include functions, roles, and the nature of credentials or privileges associated with transferred or terminated individuals.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Information Security Program Policy; DPS Security and Management Control Outsourcing Standard for Non-Channelers. **State:** DIR Security Control Standards Catalog. **Federal**: NIST SP 800-35, 800-63-3; FBI CJIS CSP v5.9	AT-2, AT-3, MA-5, PE-3, PS-2, PS-3, PS-4, PS-5, PS-6, SA-5, SA-9, SA-21.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Personnel security policy; procedures addressing external personnel security; list of personnel security requirements; acquisition documents; service-level agreements; compliance monitoring process; system security plan; other relevant documents or record.

Interview: Organizational personnel with personnel security responsibilities; external providers; system/network administrators; organizational personnel with account management responsibilities; organizational personnel with information security responsibilities.

Test: Organizational processes for managing and monitoring external personnel security; automated mechanisms supporting and/or implementing the monitoring of provider compliance.

PS-08: PERSONNEL SANCTIONS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Employ a formal sanctions process for individuals failing to comply with established information security and privacy policies and procedures; and

b. Notify personnel or roles as defined in the personnel security policy within 24 hours when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS must employ a formal sanctions process for personnel failing to comply with established information security policies and procedures. [Source: DIR Control Standards Catalog PS-8]

SUPPLEMENTAL GUIDANCE

Organizational sanctions reflect applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Sanctions processes are described in access agreements and can be included as part of general personnel policies for organizations and/or specified in security and privacy policies. Organizations consult with the Office of the General Counsel regarding matters of employee sanctions.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Information Security Program Policy; DFPS Acceptable Use Agreement. **State:** DIR Security Control Standards Catalog. **Federal**: NIST SP 800-35, 800-63-3; FBI CJIS CSP v5.9	PL-4, PM-12, PS-6, PT-1.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Personnel security policy; personnel security procedures; procedures addressing personnel sanctions; access agreements (including non-disclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements); list of personnel or roles to be notified of formal employee sanctions; records or notifications of formal employee sanctions; system security plan; privacy plan; personally identifiable information processing policy; other relevant documents or records.

Interview: Organizational personnel with personnel security responsibilities; legal counsel; organizational personnel with information security and privacy responsibilities.

Test: Organizational processes for managing formal employee sanctions; automated mechanisms supporting and/or implementing formal employee sanctions notifications.

PS-09: POSITION DESCRIPTIONS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization incorporates security and privacy roles and responsibilities into organizational position descriptions.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Include in position descriptions security and privacy roles in accordance with the access control policy and account management procedures (see AC-02).

Std.02 — Ensure that position roles are tagged for appropriate role-based training (see AT-03).

SUPPLEMENTAL GUIDANCE

Specification of security and privacy roles in individual organizational position descriptions facilitates clarity in understanding the security or privacy responsibilities associated with the roles and the role-based security and privacy training requirements for the roles.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Information Security Program Policy; DFPS Acceptable Use Agreement. **State:** DIR Security Control Standards Catalog. **Federal**: NIST SP 800-35, 800-63-3; FBI CJIS CSP v5.9	PL-4, PM-12, PS-6, PT-1.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Personnel security policy; personnel security procedures; procedures addressing position descriptions; security and privacy position descriptions; system security plan; privacy plan; privacy program plan; other relevant documents or records.

Interview: Organizational personnel with personnel security responsibilities; organizational personnel with information security and privacy responsibilities; organizational personnel with human capital management responsibilities.

Test: Organizational processes for managing position descriptions.

(PT) PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY

The relationship between security and privacy is recognized through this control. The Personally Identifiable Information Processing and Transparency control area addresses matters such as determining authorization to process or store personal information, obtaining consent, giving sufficient privacy notice, and defining a purpose within the organization for handling this information.

The intended audience for this Control includes, but is not limited to, information resource owners and custodians. The information resource owner, or their designee, is responsible for ensuring that the privacy management measures described in this Control family are implemented by personnel with

privacy management responsibilities (e.g. system/network administrators, information security analyst, etc.).

PT-01: POLICY AND PROCEDURES	
Priority: P1	
Baseline(s): Low, Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization:

a. Develop, document, and disseminate to appropriate personnel:
   1. Organization-level personally identifiable information processing and transparency policy that:
      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the personally identifiable information processing and transparency policy and the associated personally identifiable information processing and transparency controls;
b. Designate a senior management official as defined in the personally identifiable information processing and transparency policy to manage the development, documentation, and dissemination of the personally identifiable information processing and transparency policy and procedures; and
c. Review and update the current personally identifiable information processing and transparency:
   1. Policy every two (2) years and following major changes to legislation or security requirements; and
   2. Procedures every two (2) years and following major changes to legislation or security requirements.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Security requirements shall be identified, documented, and addressed in all phases of personally identifiable information processing and transparency.

Std.02 — The DFPS Chief Information Security Officer shall be responsible for:

d. Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks;
e. Providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities under 1 TAC 202; and
f. Developing and recommending policies and establishing procedures and practices, in cooperation with the agency Information Resources Manager, information-owners and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, or disclosure. [Source: 1 TAC 202.21(b)(3, 5, 8)]

SUPPLEMENTAL GUIDANCE

Personally identifiable information processing and transparency policy and procedures address the controls in the PT family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of personally identifiable information processing and transparency policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need

for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations.

Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to personally identifiable information processing and transparency policy and procedures include assessment or audit findings, breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** 1 TAC 202.21(b)(3, 5, 8). **Federal**: OMB A-130.	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Personally identifiable information processing and transparency policy and procedures; privacy plan; privacy program plan; other relevant documents or records.

Interview: Organizational personnel with personally identifiable information processing and transparency responsibilities; organizational personnel with information security and privacy responsibilities.

PT-02: AUTHORITY TO PROCESS PERSONALLY IDENTIFIABLE INFORMATION

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization:

a. Determine and document the authority, as determined in the privacy impact assessments (PIAs), that permits the collection, use, maintenance, or transmission (either generally or in support of a specific program or information system need) of personally identifiable information; and
b. Restrict the collection, use, maintenance, or transmission of personally identifiable information to only that which is authorized.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business. [Source: Bus. & Comm. 521.052(a)]

SUPPLEMENTAL GUIDANCE

The processing of personally identifiable information is an operation or set of operations that the information system or organization performs with respect to personally identifiable information across the information life cycle. Processing includes but is not limited to creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal. Processing operations also include logging, generation, and transformation, as well as analysis techniques, such as data mining.

Organizations may be subject to laws, executive orders, directives, regulations, or policies that establish the organization's authority and thereby limit certain types of processing of personally identifiable information or establish other requirements related to the processing. Organizational personnel consult with the senior agency official for privacy and legal counsel regarding such authority, particularly if the organization is subject to multiple jurisdictions or sources of authority. For organizations whose processing is not determined according to legal authorities, the organization's policies and determinations govern how they process personally identifiable information. While processing of personally identifiable information may be legally permissible, privacy risks may still arise. Privacy risk assessments can identify the privacy risks associated with the authorized processing of personally identifiable information and support solutions to manage such risks.

Organizations consider applicable requirements and organizational policies to determine how to document this authority. For federal agencies, the authority to process personally identifiable information is documented in privacy policies and notices, system of records notices, privacy impact assessments, Privacy Act statements, computer matching agreements and notices, contracts, information sharing agreements, memoranda of understanding, and other documentation.

Organizations take steps to ensure that personally identifiable information is only processed for authorized purposes, including training organizational personnel on the authorized processing of personally identifiable information and monitoring, and auditing organizational use of personally identifiable information.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** TX Govt. Code 552; Bus. & Comm. 521. **Federal**: Privacy Act; OMB A-130; NIST IR 8112.	AC-2, AC-3, CM-13, IR-9, PM-9, PM-24, PT-1, PT-3, PT-5, PT-6, RA-3, RA-8, SI-12, SI-18.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Personally identifiable information processing and transparency policy and procedures; privacy plan; other relevant documents or records.

Interview: Organizational personnel with personally identifiable information processing and transparency responsibilities; organizational personnel with information security and privacy responsibilities.

Test: Organizational processes for authorizing the processing of personally identifiable information; automated mechanisms supporting and/or implementing the restriction of personally identifiable information processing.

PT-03: AUTHORITY TO PROCESS PERSONALLY IDENTIFIABLE INFORMATION

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization:

a. Identify and document the purpose(s) as defined in PT-05 for processing personally identifiable information;

b. Describe the purpose(s) in the public privacy notices and policies of the organization;

c. Restrict the processing as defined in PT-02 of personally identifiable information to only that which is compatible with the identified purpose(s); and

d. Monitor changes in processing personally identifiable information and implement mechanisms as defined in System Security Plans (SSPs) to ensure that any changes are made in accordance with requirements as defined in the privacy policy.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Assess the privacy risk to individuals resulting from the collection of the sensitive personal information (SPI) to be collected for the processing purposes. Document this assessment in the privacy impact assessment (PIA) for each system or application.

Std.02 — Review and update PIAs as required as part of the authority to operate process (ATO).

SUPPLEMENTAL GUIDANCE

Identifying and documenting the purpose for processing provides organizations with a basis for understanding why personally identifiable information may be processed. The term "process" includes every step of the information life cycle, including creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal. Identifying and documenting the purpose of processing is a prerequisite to enabling owners and operators of the system and individuals whose information is processed by the system to understand how the information will be processed. This enables individuals to make informed decisions about their engagement with information systems and organizations and to manage their privacy interests. Once the specific processing purpose has been identified, the purpose is described in the organization's privacy notices, policies, and any related privacy compliance documentation, including privacy impact assessments, system of records notices, Privacy Act statements, computer matching notices, and other applicable Federal Register notices.

Organizations take steps to help ensure that personally identifiable information is processed only for identified purposes, including training organizational personnel and monitoring, and auditing organizational processing of personally identifiable information.

Organizations monitor for changes in personally identifiable information processing. Organizational personnel consult with the senior agency official for privacy and legal counsel to ensure that any new purposes that arise from changes in processing are compatible with the purpose for which the information was collected, or if the new purpose is not compatible, implement mechanisms in accordance with defined requirements to allow for the new processing, if appropriate. Mechanisms may include obtaining consent from individuals, revising privacy policies, or other measures to manage privacy risks that arise from changes in personally identifiable information processing purposes.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** N/A **Federal**: Privacy Act; OMB A-130; NIST IR 8112.	AC-2, AC-3, CM-13, IR-9, PM-9, PM-24, PT-1, PT-3, PT-5, PT-6, RA-3, RA-8, SI-12, SI-18.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Personally identifiable information processing and transparency policy and procedures; configuration management plan; organizational privacy notices; organizational policies; Privacy Act statements; computer matching notices; applicable Federal Register notices; documented requirements for enforcing and monitoring the processing of personally identifiable information; privacy plan; other relevant documents or records.

Interview: Organizational personnel with personally identifiable information processing and transparency responsibilities; organizational personnel with information security and privacy responsibilities.

Test: Organizational processes for authorizing the processing of personally identifiable information; automated mechanisms supporting and/or implementing the management of authorized personally identifiable information processing; organizational processes for monitoring changes in processing personally identifiable information.

PT-04: CONSENT

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization implements tools or mechanisms for individuals to consent to the processing of their personally identifiable information prior to its collection that facilitate individuals' informed decision-making.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Ensure that consent is:

a. Explicit; and
b. Auditable.

SUPPLEMENTAL GUIDANCE

Consent allows individuals to participate in making decisions about the processing of their information and transfers some of the risk that arises from the processing of personally identifiable information from the organization to an individual. Consent may be required by applicable laws, executive orders, directives, regulations, policies, standards, or guidelines. Otherwise, when selecting consent as a control, organizations consider whether individuals can be reasonably expected to understand and accept the privacy risks that arise from their authorization. Organizations consider whether other controls may more effectively mitigate privacy risk either alone or in conjunction with consent. Organizations also consider any demographic or contextual factors that may influence the understanding or behavior of individuals with respect to the processing carried out by the system or organization. When soliciting consent from individuals, organizations consider the appropriate mechanism for obtaining consent, including the type of consent (e.g., opt-in, opt-out), how to properly authenticate and identity proof individuals and how to obtain consent through electronic means. In addition, organizations consider providing a mechanism for individuals to revoke consent once it has been provided, as appropriate. Finally, organizations consider usability factors to help individuals understand the risks being accepted when providing consent, including the use of plain language, and avoiding technical jargon.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** TX Govt. Code 552. **Federal**: Privacy Act; OMB A-130; NIST SP 800-63-3.	AC-16, PT-2, PT-5.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Personally identifiable information processing and transparency policy and procedures; consent policies and procedures; consent tools and mechanisms; consent presentation or display (user interface); privacy plan; other relevant documents or records

Interview: Organizational personnel with personally identifiable information processing and transparency responsibilities; organizational personnel with information security and privacy responsibilities.

Test: Organizational processes for the collection of personally identifiable information; consent tools or mechanisms for users to authorize the processing of their personally identifiable information; automated mechanisms implementing consent.

PT-05: PRIVACY NOTICE

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization provides notice to individuals about the processing of personally identifiable information that:

a. Is available to individuals upon first interacting with an organization, and subsequently at least annually and whenever an individual updates sensitive personal information (SPI);
b. Is clear and easy-to-understand, expressing information about personally identifiable information processing in plain language;
c. Identifies the authority that authorizes the processing of personally identifiable information;
d. Identifies the purposes for which personally identifiable information is to be processed; and
e. Includes information as defined in Std.01.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — the DFPS Privacy Notice must include, at a high level suitable for the public:

a. A description of agency activities that impact privacy including its collection, use, sharing, safeguarding, maintenance and disposal of SPI;
    1. The SPI the agency collects;
    2. The routine uses of SPI;
    3. Whether the agency shares SPI externally, and if so, the purposes of that sharing; and
    4. How the agency protects SPI.
b. Authority for collecting SPI;
c. The choices individuals may have regarding how the organization uses and shares SPI;
    1. Whether individuals can rescind specific consent

2. The consequences of not supplying requested information; and
3. Contact information in case of questions, complaints, and concerns.

Std.02 — Revise the public Privacy Notice to reflect changes in practice or policy that affect SPI or changes in activities that impact privacy before or as soon as feasible after such changes.

d.

SUPPLEMENTAL GUIDANCE

Privacy notices help inform individuals about how their personally identifiable information is being processed by the system or organization. Organizations use privacy notices to inform individuals about how, under what authority, and for what purpose their personally identifiable information is processed, as well as other information such as choices individuals might have with respect to that processing and other parties with whom information is shared. Laws, executive orders, directives, regulations, or policies may require that privacy notices include specific elements or be provided in specific formats. Federal agency personnel consult with the senior agency official for privacy and legal counsel regarding when and where to provide privacy notices, as well as elements to include in privacy notices and required formats. In circumstances where laws or government-wide policies do not require privacy notices, organizational policies and determinations may require privacy notices and may serve as a source of the elements to include in privacy notices.

Privacy risk assessments identify the privacy risks associated with the processing of personally identifiable information and may help organizations determine appropriate elements to include in a privacy notice to manage such risks. To help individuals understand how their information is being processed, organizations write materials in plain language and avoid technical jargon.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** TX Govt. Code 552. **Federal**: Privacy Act; OMB A-108, A-130.	PM-20, PM-22, PT-2, PT-3, PT-4, PT-7, RA-3, SC-42, SI-18.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Personally identifiable information processing and transparency policy and procedures; privacy notice; Privacy Act statements; privacy plan; other relevant documents or records.

Interview: Organizational personnel with personally identifiable information processing and transparency responsibilities; organizational personnel with information security and privacy responsibilities.

Test: Organizational processes and implementation support or mechanisms for providing notice to individuals regarding the processing of their personally identifiable information.

PT-07 SPECIFIC CATEGORIES OF PERSONALLY IDENTIFIABLE INFORMATION

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization apply processing conditions in accordance with the DFPS Data Classification Policy for specific categories of personally identifiable information

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Establish, maintain, and update at least annually an inventory containing a listing of all programs and information systems identified as collecting, using, maintaining, or sharing sensitive personal information (SPI).

SUPPLEMENTAL GUIDANCE

Organizations apply any conditions or protections that may be necessary for specific categories of personally identifiable information. These conditions may be required by laws, executive orders, directives, regulations, policies, standards, or guidelines. The requirements may also come from the results of privacy risk assessments that factor in contextual changes that may result in an organizational determination that a particular category of personally identifiable information is particularly sensitive or raises particular privacy risks.

Organizations consult with the senior agency official for privacy and legal counsel regarding any protections that may be necessary.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Data Classification Policy; DFPS Data Classification Standard. **State:** TX Govt. Code 552. **Federal**: Privacy Act; OMB A-108, A-130; NARA CUI.	IR-9, PT-2, PT-3, RA-3.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Personally identifiable information processing and transparency policy and procedures; privacy notice; Privacy Act statements; privacy plan; other relevant documents or records.

Interview: Organizational personnel with personally identifiable information processing and transparency responsibilities; organizational personnel with information security and privacy responsibilities.

Test: Organizational processes and implementation support or mechanisms for providing notice to individuals regarding the processing of their personally identifiable information.

PT-07(01): SOCIAL SECURITY NUMBERS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

When a system processes Social Security numbers:

a. Eliminate unnecessary collection, maintenance, and use of Social Security numbers, and explore alternatives to their use as a personal identifier;

b. Do not deny any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his or her Social Security number; and
c. Inform any individual who is asked to disclose his or her Social Security number whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Provide the DFPS Privacy Notice before requesting personally identifiable information (PII) including Social Security Numbers.

SUPPLEMENTAL GUIDANCE

Federal law and policy establish specific requirements for organizations' processing of Social Security numbers. Organizations take steps to eliminate unnecessary uses of Social Security numbers and other sensitive information and observe any particular requirements that apply.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Privacy Policy. **State:** TX Govt. Code 552. **Federal**: Privacy Act; OMB A-108, A-130.	IR-9, PT-2, PT-3, RA-3.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Personally identifiable information processing and transparency policy and procedures; privacy notice; Privacy Act statements; privacy plan; other relevant documents or records.

Interview: Organizational personnel with personally identifiable information processing and transparency responsibilities; organizational personnel with information security and privacy responsibilities.

Test: Organizational processes for identifying, reviewing, and taking action to control the unnecessary use of Social Security numbers; implementation of an alternative to Social Security numbers as identifiers.

(RA) RISK ASSESSMENT

DFPS requires that an understanding of the agency's cybersecurity risk to operations (including mission, functions, image, or reputation), organizational assets, and individuals is assessed.

The intended audience for this Control includes, but is not limited to, information resource owners and custodians. The information resource owner, or their designee, is responsible for ensuring that the risk management measures described in this Control family are implemented by personnel with risk management responsibilities (e.g. system/network administrators, information security analyst, etc.).

RA-01: RISK ASSESSMENT POLICY AND PROCEDURES

Priority: P1	
Baseline(s): Low, Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization:

a. Develop, document, and disseminate to appropriate personnel:

1. Organization-level risk assessment policy that:

a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls;

b. Designate a senior management official as defined in the risk assessment policy to manage the development, documentation, and dissemination of the risk assessment policy and procedures; and

c. Review and update the current risk assessment:

1. Policy every year and following major changes to legislation or security requirements; and

3. Procedures every year and following major changes to legislation or security requirements.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS must have a risk assessment policy which includes process of identifying, evaluating, and documenting the level of impact that may result from the operation of an information system on an organization's mission, functions, image, reputation, assets, or individuals. [Source: DIR Control Standards Catalog RA-1]

Std.02 — The information owner or his or her designated representative(s) are responsible for classifying information under their authority, with the concurrence of the state agency head or his or her designated representative(s), in accordance with DFPS's established information classification categories; approving access to information resources and periodically review access lists based on documented risk management decisions; formally assigning custody of information or an information resource; coordinating data security control requirements with the CISO; conveying data security control requirements to custodians; providing authority to custodians to implement security controls and procedures; justifying, documenting, and being accountable for exceptions to security controls. The information owner shall coordinate and obtain approval for exceptions to security controls with the agency information security officer; and participating in risk assessments as provided under 1 TAC 202.25. [Source: 1 TAC 202.22(1)]

Std.03 — Custodians of information resources, including third party entities providing outsourced information resources services to state agencies shall implement controls required to protect information and information resources required by this chapter based on the classification and risks specified by the information owner(s) or as specified by the policies, procedures, and standards defined by the agency information security program; provide owners with information to evaluate the cost-effectiveness of controls and monitoring; adhere to monitoring techniques and procedures, approved by the ISO, for detecting, reporting, and investigating incidents; provide information necessary to provide appropriate information security training to employees; and ensure information is recoverable in accordance with risk management decisions. [Source: 1 TAC 202.22(2)]

Std.04 — The user of an information resource has the responsibility to use the resource only for the purpose specified by the agency or information-owner; comply with information security controls and agency policies to prevent unauthorized or accidental disclosure, modification, or destruction; and formally acknowledge that they will comply with the security policies and procedures in a method determined by the agency head or his or her designated representative. [Source: 1 TAC 202.22(3)]

Std.05 — Agency information resources designated for use by the public shall be configured to enforce security policies and procedures without requiring user participation or intervention. Information resources must require the acceptance of a banner or notice prior to use. [Source: 1 TAC 202.22(4)]

Std.06 — The DFPS Chief Information Security Officer shall be responsible for:

a. Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks;

b. Providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities under 1 TAC 202; and

c. Developing and recommending policies and establishing procedures and practices, in cooperation with the agency Information Resources Manager, information-owners and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, or disclosure. [Source: 1 TAC 202.21(b)(3, 5, 8)]

Std.07 — The agency must, in consultation with the agency Information Resource Manager (IRM) and Chief Information Security Officer (CISO), identify information owners, custodians, and users of information resources.

Std.08 — The information owners', custodians', and users' responsibilities must be defined and documented by the agency.

SUPPLEMENTAL GUIDANCE

Risk assessment policy and procedures address the controls in the RA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of risk assessment policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies reflecting the complex nature of organizations.

Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to risk assessment policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Information Risk Management Policy. **State:** 1 TAC 202.22(1, 2); DIR Security Control Standards Catalog. **Federal**: OMB A-130; NIST SP 800-12, 800-30, 800-39, 800-100.	PM-9, PS-8, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Risk assessment policy and procedures; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with risk assessment responsibilities; organizational personnel with security and privacy responsibilities.

RA-02: SECURITY CATEGORIZATION

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization:

a. Categorize the system and information it processes, stores, and transmits;

b. Document the security categorization results, including supporting rationale, in the security plan for the system; and

c. Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS is responsible for defining all information classification categories except the Confidential or Regulated Information category, which is defined in Subchapter A of 1 TAC 202, and establishing the controls for each. [Source: 1 TAC 202.24(b)(1)]

Std.02 — The Information Owner or his or her designated representative(s) are responsible for classifying information under their authority, with the concurrence of the DFPS Commissioner or his or her designated representative(s), in accordance with agency's established information classification categories. [Source: 1 TAC 202.22(1)(A)]

Std.03 — Involve the Senior Official for Privacy, or their designee, when conducting the security categorization process for information systems containing personally identifiable information (PII) or sensitive personal information (SPI).

SUPPLEMENTAL GUIDANCE

Security categories describe the potential adverse impacts or negative consequences to organizational operations, organizational assets, and individuals if organizational information and systems are compromised through a loss of confidentiality, integrity, or availability. Security categorization is also a type of asset loss characterization in systems security engineering processes that is carried out throughout the system development life cycle. Organizations can use privacy risk assessments or privacy impact assessments to better understand the potential adverse effects on individuals. CNSSI 1253 provides additional guidance on categorization for national security systems.

Organizations conduct the security categorization process as an organization-wide activity with the direct involvement of chief information officers, senior agency information security officers, senior agency officials for privacy, system owners, mission and business owners, and information owners or stewards. Organizations

consider the potential adverse impacts to other organizations and, in accordance with USA Patriot Act and Homeland Security Presidential Directives, potential national-level adverse impacts.

Security categorization processes facilitate the development of inventories of information assets and, along with CM-08, mappings to specific system components where information is processed, stored, or transmitted. The security categorization process is revisited throughout the system development life cycle to ensure that the security categories remain accurate and relevant.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** 1 TAC 202.22(1)(A), 1 TAC 202.24(b)(1); DIR Security Control Standards Catalog **Federal**: FIPS 199, 200; NIST SP 800-30, 800-37, 800-39, 800-60-1, 800-60-2, 800-160-1; CNSSI 1253; NARA CUI.	CM-8, MP-4, PL-2, PL-10, PL-11, PM-7, RA-3, RA-5, RA-7, RA-8, SA-8, SC-7, SC-38, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Personally identifiable information processing and transparency policy and procedures; privacy plan; other relevant documents or records.

Interview: Organizational personnel with personally identifiable information processing and transparency responsibilities; organizational personnel with information security and privacy responsibilities.

Test: Organizational processes for authorizing the processing of personally identifiable information; automated mechanisms supporting and/or implementing the restriction of personally identifiable information processing.

RA-03: RISK ASSESSMENT

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization:

a. Conduct a risk assessment, including:
   1. Identifying threats to and vulnerabilities in the system;
   2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and
   3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;
b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;
c. Document risk assessment results in organization approved assessment report format;
d. Review risk assessment results annually;
e. Disseminate risk assessment results to Information Owners, Information Custodians,

f. Information Security Office; and

g. Update the risk assessment annually or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Risk assessment results, vulnerability reports, and similar information shall be documented and presented to the DFPS Commissioner or his or her designated representative(s). The DFPS Commissioner or his or her designated representative(s) shall make the final risk management decisions to either accept exposures or protect the data according to its value/sensitivity. The DFPS Commissioner or his or her designated representative(s) shall approve the security risk management plan. This information may be exempt from disclosure under Sec. 2054.077(c), Government Code. [Source: DIR Control Standards Catalog RA-3]

Std.02 — The DFPS Chief Information Security Officer shall be responsible for ensuring that annual information security risk assessments are performed and documented by information- owners. [Source: 1 TAC 202.21(b)(6)]

Std.03 — An agency-wide information security program must be approved by the agency head and include periodic assessments of the risk and impact that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency. [Source: 1 TAC 202.24(a)(1)]

Std.04 — A risk assessment of DFPS information and information systems shall be performed and documented. The inherent impact will be ranked, at a minimum, as either "High," "Moderate," or "Low." The frequency of the future risk assessments will be documented. Risk assessment results, vulnerability reports, and similar information shall be documented and presented to the Information Security Officer or his or her designated representative(s). [Source: 1 TAC 202.25(1, 2, 3)]

SUPPLEMENTAL GUIDANCE

Risk assessments consider threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the Nation. Risk assessments also consider risk from external parties, including contractors who operate systems on behalf of the organization, individuals who access organizational systems, service providers, and outsourcing entities.

Organizations can conduct risk assessments at all three levels in the risk management hierarchy (i.e., organization level, mission/business process level, or information system level) and at any stage in the system development life cycle. Risk assessments can also be conducted at various steps in the Risk Management Framework, including preparation, categorization, control selection, control implementation, control assessment, authorization, and control monitoring. Risk assessment is an ongoing activity carried out throughout the system development life cycle.

Risk assessments can also address information related to the system, including system design, the intended use of the system, testing results, and supply chain-related information or artifacts. Risk assessments can play an important role in control selection processes, particularly during the application of tailoring guidance and in the earliest phases of capability determination.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** 1 TAC 202.21(b)(6), 1 TAC 202.24(a)(1), 1 TAC 202.25(1, 2, 3); DIR Security Control Standards Catalog.	CM-8, MP-4, PL-2, PL-10, PL-11, PM-7, RA-3, RA-5, RA-7, RA-8, SA-8, SC-7, SC-38, SI-12.

Federal: OMB A-130; NIST SP 800-30, 800-39, 800-161; NIST IR 8023, 8062, 8272; FBI CJIS CSP v5.9.	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Risk assessment policy; risk assessment procedures; security and privacy planning policy and procedures; procedures addressing organizational assessments of risk; risk assessment; risk assessment results; risk assessment reviews; risk assessment updates; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with risk assessment responsibilities; organizational personnel with security and privacy responsibilities.

Test: Organizational processes for risk assessment; automated mechanisms supporting and/or for conducting, documenting, reviewing, disseminating, and updating the risk assessment.

RA-03(01): SUPPLY CHAIN RISK ASSESSMENT

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization:

a. Assess supply chain risks associated with all systems, system components, and system services under configuration management; and

b. Update the supply chain risk assessment at least annually, when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Supply chain-related events include disruption, use of defective components, insertion of counterfeits, theft, malicious development practices, improper delivery practices, and insertion of malicious code. These events can have a significant impact on the confidentiality, integrity, or availability of a system and its information and, therefore, can also adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. The supply chain-related events may be unintentional or malicious and can occur at any point during the system life cycle. An analysis of supply chain risk can help an organization identify systems or components for which additional supply chain risk mitigations are required.

REFERENCES	**RELATED CONTROLS**

Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; NIST SP 800-30, 800-39, 800-161; NIST IR 8023, 8062, 8272.	RA-2, RA-9, PM-17, PM-30, SR-2.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Supply chain risk management policy; inventory of critical systems, system components, and system services; risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of supply chain risk; risk assessment; risk assessment results; risk assessment reviews; risk assessment updates; acquisition policy; system security plan; supply chain risk management plan; other relevant documents or records.

Interview: Organizational personnel with risk assessment responsibilities; organizational personnel with security responsibilities; organizational personnel with supply chain risk management responsibilities.

Test: Organizational processes for risk assessment; automated mechanisms supporting and/or for conducting, documenting, reviewing, disseminating, and updating the supply chain risk assessment.

RA-05: VULNERABILITY SCANNING

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

c. Monitor and scan for vulnerabilities in the system and hosted applications in accordance with Std.06 and when new vulnerabilities potentially affecting the system are identified and reported;

d. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

   1. Enumerating platforms, software flaws, and improper configurations;
   2. Formatting checklists and test procedures; and
   3. Measuring vulnerability impact;

e. Analyze vulnerability scan reports and results from vulnerability monitoring;

f. Remediate legitimate vulnerabilities per the timeline outlined in Std.07 in accordance with an organizational assessment of risk;

g. Share information obtained from the vulnerability monitoring process and control assessments with the Information Owner, and in accordance with Stds.02, 03, & 05 to help eliminate similar vulnerabilities in other systems; and

h. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS, when implementing an Internet website or mobile application that processes any sensitive personal or personally identifiable information or confidential information, must subject the website or application to a vulnerability and penetration test and address any vulnerability identified in the test. [Source: TX Govt. Code 2054.516(a)(2)]

Std.02 — The DFPS Chief Information Security Officer shall prepare or have prepared a report, including an executive summary of the findings of the biennial report, not later than October 15 of each even-numbered year, assessing the extent to which a computer, a computer program, a computer network, a computer system, a printer, an interface to a computer system, including mobile and peripheral devices, computer software, or data processing of the agency or of a contractor of the agency is vulnerable to unauthorized access or harm, including the extent to which the agency's or contractor's electronically stored information is vulnerable to alteration, damage, erasure, or inappropriate use. [Source: TX Govt. Code 2054.077(b)]

Std.03 — Except as provided by TX Govt. Code 2054.077, a vulnerability report and any information or communication prepared or maintained for use in the preparation of a vulnerability report is confidential or regulated and is not subject to disclosure under Chapter 552. [Source: TX Govt. Code 2054.077(c)]
Std.04 — The DFPS Chief Information Security Officer shall provide an electronic copy of the vulnerability report on its completion to:

a. The Department of Information Resources;
b. The state auditor;
c. DFPS Commissioner
d. The agency's designated information resources manager; and
e. Any other information technology security oversight group specifically authorized by the legislature to receive the report. [Source: TX Govt. Code 2054.077(d)]

Std.05 — Separate from the executive summary described by Subsection (b), DFPS shall prepare a summary of the agency's vulnerability report that does not contain any information the release of which might compromise the security of the state agency's or state agency contractor's computers, computer programs, computer networks, computer systems, printers, interfaces to computer systems, including mobile and peripheral devices, computer software, data processing, or electronically stored information. The summary is available to the public on request. [Source: TX Govt. Code 2054.077(e)]

Std.06 — Conduct scans according to the Scan Frequency schedule:

a. At least once per week, perform:
    1. Credentialed scans on internet-facing networked assets;
    2. Uncredentialed scans on all internet-facing networked assets.
b. At least once per month, perform credentialed scans on internal networked assets

Std.07 — Remediate legitimate vulnerabilities as defined in the DFPS Vulnerability Management Policy with the timeline beginning from the date of identification by a vulnerability scanner.

Std.08 — Utilize an up-to-date SCAP-compliant vulnerability scanning tool. [Source: CIS 3.1]

Std.09 — The network and host-based vulnerability scanner shall provide the following capabilities:

a. Identify active hosts on networks;
b. Identify active and vulnerable services (ports) on hosts;
c. Identify vulnerabilities associated with discovered operating systems and applications. [Source: FedRAMP Vulnerability Scanning Requirements]

Std.10 — Where possible, use tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to test for the presence of vulnerabilities. [Source: FedRAMP Vulnerability Scanning Requirements]

Std.11 — DFPS uses the latest Common Vulnerability Scoring System (CVSS) framework for ranking vulnerability criticality. All vulnerability scanning tools must support this framework.

SUPPLEMENTAL GUIDANCE

Security categorization of information systems guides the frequency and comprehensiveness of vulnerability scans. Organizations determine the required vulnerability scanning for all information system components, ensuring that potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked. Vulnerability analyses for custom software applications may require additional approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Vulnerability scanning includes, for example: (i) scanning for patch levels; (ii) scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and (iii) scanning for improperly configured or incorrectly operating information flow control mechanisms. Organizations consider using tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to determine/test for the presence of vulnerabilities. Suggested sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD). In addition, security control assessments such as red team exercises provide other sources of potential vulnerabilities for which to scan. Organizations also consider using tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS).

For dynamic application security testing (DAST), see SA-11(08).

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Vulnerability Management Policy. **State:** 1 TAC 202.21(b)(6), 1 TAC 202.24(a)(1), 1 TAC 202.25(1, 2, 3); DIR Security Control Standards Catalog. **Federal**: ISO 29147; NIST SP 800-40, 800-53A, 800-70, 800-115, 800-126; NIST IR 7788, 8011-4, 8023; FBI CJIS CSP v5.9.	CA-2, CA-7, CA-8, CM-2, CM-4, CM-6, CM-8, RA-2, RA-3, SA-11, SA-15, SC-38, SI-2, SI-3, SI-4, SI-7, SR-11.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; assessment report; vulnerability scanning tools and associated configuration documentation; vulnerability scanning results; patch and vulnerability management records; system security plan; other relevant documents or records.

Interview: Organizational personnel with risk assessment, control assessment, and vulnerability scanning responsibilities; organizational personnel with vulnerability scan analysis responsibilities; organizational personnel with vulnerability remediation responsibilities; organizational personnel with security responsibilities; system/network administrators.

Test: Organizational processes for vulnerability scanning, analysis, remediation, and information sharing; automated mechanisms supporting and/or implementing vulnerability scanning, analysis, remediation, and information sharing.

RA-05(01): UPDATE TOOL CAPABILITY

Priority: P1	
Baseline(s): Low, Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

This control is withdrawn and incorporated into RA-05 but still referenced in the FBI CJIS Security Policy v5.9. Please see RA-05.

RA-05(02): UPDATE BY FREQUENCY / PRIOR TO NEW SCAN / WHEN IDENTIFIED

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization updates the system vulnerabilities to be scanned weekly, prior to a new scan, and when new vulnerabilities are identified and reported.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS employs automated mechanisms to immediately update the vulnerability scanner when new vulnerabilities are identified and reported.

SUPPLEMENTAL GUIDANCE

Due to the complexity of modern software, systems, and other factors, new vulnerabilities are discovered on a regular basis. It is important that newly discovered vulnerabilities are added to the list of vulnerabilities to be scanned to ensure that the organization can take steps to mitigate those vulnerabilities in a timely manner.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Vulnerability Management Policy. **State:** DIR Security Control Standards Catalog. **Federal**: ISO 29147; NIST SP 800-40, 800-53A, 800-70, 800-115, 800-126; NIST IR 7788, 8011-4, 8023; FBI CJIS CSP v5.9.	SI-5.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Procedures addressing vulnerability scanning; assessment report; vulnerability scanning tools and associated configuration documentation; vulnerability scanning results; patch and vulnerability management records; system security plan; other relevant documents or records.

Interview: Organizational personnel with vulnerability scanning responsibilities; organizational personnel with vulnerability scan analysis responsibilities; organizational personnel with security responsibilities; system/network administrators.

Test: Organizational processes for vulnerability scanning; automated mechanisms/tools supporting and/or implementing vulnerability scanning.

RA-05(03): BREADTH / DEPTH OF COVERAGE

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization employs vulnerability scanning procedures that can identify the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked).

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Agencies shall monitor mobile devices to ensure their patch and update state is current. [Source: FBI CJIS CSP v5.9]

SUPPLEMENTAL GUIDANCE

Based on the varying connection methods for mobile devices, an always on connection cannot be guaranteed for patching and updating. Devices without always-on cellular connections may not be reachable for extended periods of time by the MDM or solution either to report status or initiate patching.

The breadth of vulnerability scanning coverage can be expressed as a percentage of components within the system, by the particular types of systems, by the criticality of systems, or by the number of vulnerabilities to be checked. Conversely, the depth of vulnerability scanning coverage can be expressed as the level of the system design that the organization intends to monitor (e.g., component, module, subsystem, element). Organizations can determine the sufficiency of vulnerability scanning coverage with regard to its risk tolerance and other factors. Scanning tools and how the tools are configured may affect the depth and coverage. Multiple scanning tools may be needed to achieve the desired depth and coverage. NISP SP 800-53A provides additional information on the breadth and depth of coverage.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Vulnerability Management Policy. **State:** DIR Security Control Standards Catalog. **Federal**: NISP SP 800-53A; FBI CJIS CSP v5.9.	None.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Procedures addressing vulnerability scanning; assessment report; vulnerability scanning tools and associated configuration documentation; vulnerability scanning results; patch and vulnerability management records; system security plan; other relevant documents or records.

Interview: Organizational personnel with vulnerability scanning responsibilities; organizational personnel with vulnerability scan analysis responsibilities; organizational personnel with security responsibilities.

Test: Organizational processes for vulnerability scanning; automated mechanisms/tools supporting and/or implementing vulnerability scanning.

RA-05(04): DISCOVERABLE INFORMATION

Priority: P1

Baseline(s): High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization determines what information about the information system is discoverable by adversaries and subsequently takes take corrective actions as defined in Std.01.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Corrective actions depend on System Development Life Cycle (SDLC) phase:

a. For systems in development, require that developers make changes to system to mitigate risk; and

b. For systems in the operational & maintenance phase, implement corrective actions and document in the plan of action and milestones document (POAM).

Std.02 — Update System Security Plans (SSPs) following corrective actions.

SUPPLEMENTAL GUIDANCE

Discoverable information includes information that adversaries could obtain without compromising or breaching the system, such as by collecting information that the system is exposing or by conducting extensive web searches. Corrective actions include notifying appropriate organizational personnel, removing designated information, or changing the system to make the designated information less relevant or attractive to adversaries. This enhancement excludes intentionally discoverable information that may be part of a decoy capability (e.g., honeypots, honeynets, or deception nets) deployed by the organization.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Vulnerability Management Policy. **State:** DIR Security Control Standards Catalog. **Federal**: ISO 29147; NIST SP 800-40, 800-53A, 800-70, 800-115, 800-126; NIST IR 7788, 8011-4, 8023.	AU-13, SC-26.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Procedures addressing vulnerability scanning; assessment report; penetration test results; vulnerability scanning results; risk assessment report; records of corrective actions taken; incident response records; audit records; system security plan; other relevant documents or records.

Interview: Organizational personnel with vulnerability scanning and/or penetration testing responsibilities; organizational personnel with vulnerability scan analysis responsibilities; organizational personnel responsible for risk response; organizational personnel responsible for incident management and response; organizational personnel with security responsibilities.

Test: Organizational processes for vulnerability scanning; organizational processes for risk response; organizational processes for incident management and response; automated mechanisms/tools supporting and/or implementing vulnerability scanning; automated mechanisms supporting and/or implementing risk response; automated mechanisms supporting and/or implementing incident management and response.

RA-05(05): PRIVILEGED ACCESS

Priority: P1

Baseline(s): Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

The information system implements privileged access authorization to Sensitive, Confidential, or Controlled components for vulnerability scanning activities.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - Automated scanning tool functionality must be compliant with DFPS requirements to include the ability to perform credentialed scans.

Std.02 - Credentialed scanning must be performed on all information systems and network devices (including appliances). [Source: DFPS Vulnerability Management Policy]

Std.03 - Scanning technologies work best by performing checks directly on the systems. A service account with appropriate privileges may be needed for these tools to work effectively. DFPS must provide and maintain service accounts to support credential scanning as needed. [Source: DFPS Vulnerability Management Policy]

Std.04 - Restrict access to vulnerability scanning functionality and information to system owners, authorized system administrators, designated security officials, and others with a valid business need.

SUPPLEMENTAL GUIDANCE

In certain situations, the nature of the vulnerability scanning may be more intrusive, or the system component that is the subject of the scanning may contain classified or controlled unclassified information, such as personally identifiable information. Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and protects the sensitive nature of such scanning.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Vulnerability Management Policy.	None.

State: DIR Security Control Standards Catalog. **Federal**: ISO 29147; NIST SP 800-40, 800-53A, 800-70, 800-115, 800-126; NIST IR 7788, 8011-4, 8023.	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Risk assessment policy; procedures addressing vulnerability scanning; system design documentation; system configuration settings and associated documentation; list of system components for vulnerability scanning; personnel access authorization list; authorization credentials; access authorization records; system security plan; other relevant documents or record.

Interview: Organizational personnel with vulnerability scanning responsibilities; system/network administrators; organizational personnel responsible for access control to the system; organizational personnel responsible for configuration management of the system; system developers; organizational personnel with security responsibilities.

Test: Organizational processes for vulnerability scanning; organizational processes for access control; automated mechanisms supporting and/or implementing access control; automated mechanisms/tools supporting and/or implementing vulnerability scanning.

RA-05(11): PUBLIC DISCLOSURE PROGRAM

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Publish a vulnerability disclosure program policy statement to a publicly accessible agency website, including reporting contact details.

Std.02 — Configure reporting channels to notify appropriate personnel.

SUPPLEMENTAL GUIDANCE

Liability Exemption. A person who in good faith discloses to a state agency or other governmental entity information regarding a potential security issue with respect to the agency's or entity's information resources technologies is not liable for any civil damages resulting from disclosing the information unless the person stole, retained, or sold any data obtained as a result of the security issue. [Source: TX Govt. Code 2054.602]

The reporting channel is publicly discoverable and contains clear language authorizing good- faith research and the disclosure of vulnerabilities to the organization. The organization does not condition its authorization on an

expectation of indefinite non-disclosure to the public by the reporting entity but may request a specific time period to properly remediate the vulnerability.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Vulnerability Management Policy. **State:** TX Govt. Code 2054.602; DIR Security Control Standards Catalog. **Federal**: ISO 29147; NIST SP 800-40, 800-53A, 800-70, 800-115, 800-126; NIST IR 7788, 8011-4, 8023.	None.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; vulnerability scanning tools and techniques documentation; vulnerability scanning results; vulnerability management records; audit records; public reporting channel; system security plan; other relevant documents or records.

Interview: Organizational personnel with vulnerability scanning responsibilities; organizational personnel with vulnerability scan analysis responsibilities; organizational personnel with security responsibilities.

Test: Organizational processes for vulnerability scanning; automated mechanisms/tools supporting and/or implementing vulnerability scanning; automated mechanisms implementing public reporting of vulnerabilities.

RA-07: RISK RESPONSE

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): Privacy

CONTROL REQUIREMENTS

Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Identify, prioritize, and implement responses to risks identified from assessments, monitoring, and audits. [Source: NIST Privacy Framework ID.RA-P5]

Std.02 — Document all responses to findings from internal assessments and monitoring in Plans of Action and Milestones (POAMs). Document all responses to findings from audits in management action plans (MAPs) and POAMs as appropriate.

SUPPLEMENTAL GUIDANCE

Organizations have many options for responding to risk including mitigating risk by implementing new controls or strengthening existing controls, accepting risk with appropriate justification or rationale, sharing, or transferring risk, or avoiding risk. The risk tolerance of the organization influences risk response decisions and actions. Risk response addresses the need to determine an appropriate response to risk before generating a plan

of action and milestones entry. For example, the response may be to accept risk or reject risk, or it may be possible to mitigate the risk immediately so that a plan of action and milestones entry is not needed. However, if the risk response is to mitigate the risk, and the mitigation cannot be completed immediately, a plan of action and milestones entry is generated.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Security Risk Standard. **State:** None. **Federal**: FIPS 199, 200; NIST SP 800-30, 800-37, 800-39, 800-160-1.	CA-5, IR-9, PM-4, PM-28, RA-2, RA-3, SR-2.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Risk assessment policy; assessment reports; audit records/event logs; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with assessment and auditing responsibilities; system/network administrators; organizational personnel with security and privacy responsibilities.

Test: Organizational processes for assessments and audits; automated mechanisms/tools supporting and/or implementing assessments and auditing.

RA-08: PRIVACY IMPACT ASSESSMENTS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): Privacy

CONTROL REQUIREMENTS

The organization conducts privacy impact assessments for systems, programs, or other activities before:

a. Developing or procuring information technology that processes personally identifiable information; and

b. Initiating a new collection of personally identifiable information that:

   1. Will be processed using information technology; and
   2. Includes personally identifiable information permitting the physical or virtual (online) contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, ten or more individuals, other than agencies, instrumentalities, or employees of the federal government

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Ensure that privacy impact assessments (PIAs) are conducted before processing of sensitive personal information (SPI).

SUPPLEMENTAL GUIDANCE

A privacy impact assessment is an analysis of how personally identifiable information is handled to ensure that handling conforms to applicable privacy requirements, determine the privacy risks associated with an information system or activity, and evaluate ways to mitigate privacy risks. A privacy impact assessment is both an analysis and a formal document that details the process and the outcome of the analysis.

Organizations conduct and develop a privacy impact assessment with sufficient clarity and specificity to demonstrate that the organization fully considered privacy and incorporated appropriate privacy protections from the earliest stages of the organization's activity and throughout the information life cycle. In order to conduct a meaningful privacy impact assessment, the organization's senior agency official for privacy works closely with program managers, system owners, information technology experts, security officials, counsel, and other relevant organization personnel. Moreover, a privacy impact assessment is not a time- restricted activity that is limited to a particular milestone or stage of the information system or personally identifiable information life cycles. Rather, the privacy analysis continues throughout the system and personally identifiable information life cycles. Accordingly, a privacy impact assessment is a living document that organizations update whenever changes to the information technology, changes to the organization's practices, or other factors alter the privacy risks associated with the use of such information technology.

To conduct the privacy impact assessment, organizations can use security and privacy risk assessments. Organizations may also use other related processes that may have different names, including privacy threshold analyses. A privacy impact assessment can also serve as notice to the public regarding the organization's practices with respect to privacy. Although conducting and publishing privacy impact assessments may be required by law, organizations may develop such policies in the absence of applicable laws. For federal agencies, privacy impact assessments may be required by E-Government Act; agencies should consult with their senior agency official for privacy and legal counsel on this requirement and be aware of the statutory exceptions and OMB guidance relating to the provision.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Security Risk Standard. **State:** None. **Federal**: E-Government Act; OMB A-130, M-03-22.	CM-4, CM-9, CM-13, PT-2, PT-3, PT-5, RA-1, RA-2, RA-3, RA-7.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Risk assessment policy; security and privacy risk assessment reports; acquisitions documents; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with assessment and auditing responsibilities; system/network administrators; system developers; program managers; legal counsel; organizational personnel with security and privacy responsibilities.

Test: Organizational processes for assessments and audits; automated mechanisms/tools supporting and/or implementing assessments and auditing.

RA-09 CRITICALITY ANALYSIS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): Privacy

CONTROL REQUIREMENTS

Identify critical system components and functions by performing a criticality analysis for all systems, system components, or system services under configuration management at all decision points as defined in DFPS system development life cycle.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Define and document in the System Security Plan (SSP) all critical hardware and software systems, system components, and system services. [Source: Catalog of Control Systems Security: Recommendations for Standards Developers]

Std.02 — For systems in the architectural design process step, perform component-level security categorization to support the system-level criticality analysis. [Source: SP 800-161]

SUPPLEMENTAL GUIDANCE

Not all system components, functions, or services necessarily require significant protections. For example, criticality analysis is a key tenet of supply chain risk management and informs the prioritization of protection activities. The identification of critical system components and functions considers applicable laws, executive orders, regulations, directives, policies, standards, system functionality requirements, system and component interfaces, and system and component dependencies. Systems engineers conduct a functional decomposition of a system to identify mission-critical functions and components. The functional decomposition includes the identification of organizational missions supported by the system, decomposition into the specific functions to perform those missions, and traceability to the hardware, software, and firmware components that implement those functions, including when the functions are shared by many components within and external to the system.

The operational environment of a system or a system component may impact the criticality, including the connections to and dependencies on cyber-physical systems, devices, system-of-systems, and outsourced IT services. System components that allow unmediated access to critical system components or functions are considered critical due to the inherent vulnerabilities that such components create. Component and function criticality are assessed in terms of the impact of a component or function failure on the organizational missions that are supported by the system that contains the components and functions.

Criticality analysis is performed when an architecture or design is being developed, modified, or upgraded. If such analysis is performed early in the system development life cycle, organizations may be able to modify the system design to reduce the critical nature of these components and functions, such as by adding redundancy or alternate paths into the system design. Criticality analysis can also influence the protection measures required by development contractors. In addition to criticality analysis for systems, system components, and system services, criticality analysis of information is an important consideration. Such analysis is conducted as part of security categorization in RA-2.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Security Risk Standard. **State:** None. **Federal**: NIST IR 8179.	CP-2, PL-2, PL-8, PL-11, PM-1, PM-11, RA-2, SA-8, SA-15, SA-20, SR-5.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Risk assessment policy; assessment reports; criticality analysis/finalized criticality for each component/subcomponent; audit records/event logs; analysis reports; system security plan; other relevant documents or records.

Interview: Organizational personnel with assessment and auditing responsibilities; organizational personnel with criticality analysis responsibilities; system/network administrators; organizational personnel with security responsibilities.

Test: Organizational processes for assessments and audits; automated mechanisms/tools supporting and/or implementing assessments and auditing.

RA-10: THREAT HUNTING

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization:

a. Establish and maintain a cyber threat hunting capability to:
   1. Search for indicators of compromise in organizational systems; and
   2. Detect, track, and disrupt threats that evade existing controls; and

b. Employ the threat hunting capability [Assignment: organization-defined frequency].

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Develop threat hunting methodologies as part of the agency-wide information security program in accordance with PM-01.

a. Threat Hunting activites should include searching for indications of compromise including unusual network traffic, unusual file changes, and the presence of malicious code.
b. The DFPS Office of Information Security may utilize external data enrichment sources, like Open-Source Intelligence (OSINT) information feeds, tools and techniques, to proactively find, collect, and analyze data regarding new and emergine cyber threats.

Std.02 — When technically feasible, integrate threat hunting capabilities and feeds into a centeral interface and/or platform (i.e. SIEM) for incident responders and threat hunters.

Std.04 — Provide role-based training to personnel assigned threat hunting roles in accordance with AT-03.

Std.05 – Include threat emulation exersizes as part of contingency planning in accordance with CP-03(01).

SUPPLEMENTAL GUIDANCE

Threat hunting is an active means of cyber defense in contrast to traditional protection measures, such as firewalls, intrusion detection and prevention systems, quarantining malicious code in sandboxes, and Security Information and Event Management technologies and systems. Cyber threat hunting involves proactively searching organizational systems, networks, and infrastructure for advanced threats. The objective is to track and disrupt cyber adversaries as early as possible in the attack sequence and to measurably improve the speed and accuracy of organizational responses. Indications of compromise include unusual network traffic, unusual file changes, and the presence of malicious code. Threat hunting teams leverage existing threat intelligence and may create new threat intelligence, which is shared with peer organizations, Information Sharing and Analysis

Organizations (ISAO), Information Sharing and Analysis Centers (ISAC), and relevant government departments and agencies.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Security Risk Standard. **State:** None. **Federal**: NIST IR 8179.	CA-2, CA-7, CA-8, RA-3, RA-5, RA-6, SI-4.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Risk assessment policy; assessment reports; audit records/event logs; threat hunting capability; system security plan; other relevant documents or records.

Interview: Organizational personnel with threat hunting responsibilities; system/network administrators; organizational personnel with security responsibilities.

Test: Organizational processes for assessments and audits; automated mechanisms/tools supporting and/or implementing threat hunting capabilities.

(SA) SYSTEM AND SERVICES ACQUISITION

DFPS requires sufficient allocation of resources to adequately protect the agency's information systems. DFPS employs a system development life cycle processes that incorporates information security considerations, system documentation, development configuration management controls, and developer security testing and evaluations. DFPS also employs software usage and installation restrictions and requires that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from DFPS.

The intended audience for this Control includes but is not limited to all information owners, managers, system administrators, and all users of DFPS information resources (i.e. full-time and contracted staff).

SA-01: SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization:

a. Develop, document, and disseminate to appropriate personnel:

   1. Organization-level system and services acquisition policy that:

      a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls;

b. Designate a senior management official as defined in the system and services acquisition policy to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; and

c. Review and update the current system and services acquisition:

1. Policy every year and following major changes to legislation or security requirements; and

2. Procedures every year and following major changes to legislation or security requirements.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Security requirements shall be identified, documented, and addressed in all phases of development or acquisition of information resources. [Source: DIR Control Standards Catalog SA-1]

Std.02 — The DFPS Information Security Officer shall be responsible for:

a. Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks;

b. Providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities under 1 TAC 202; and

c. Developing and recommending policies and establishing procedures and practices, in cooperation with the agency Information Resources Manager, information-owners and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, or disclosure. [Source: 1 TAC 202.21(b)(3, 5, 8)]

SUPPLEMENTAL GUIDANCE

System and services acquisition policy and procedures address the controls in the SA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of system and services acquisition policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to system and services acquisition policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Information Risk Management Policy; DFPS Secure System and Software Development Life Cycle Standard. **State:** 1 TAC 202.22(1, 2); DIR Security Control Standards Catalog. **Federal**: OMB A-130; NIST SP 800-12, 800-30, 800-39, 800-100, 800-160-1.	PM-9, PS-8, SA-8, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and services acquisition policy; system and services acquisition procedures; supply chain risk management policy; supply chain risk management procedures; supply chain risk management plan; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with system and services acquisition responsibilities; organizational personnel with information security and privacy responsibilities; organizational personnel with supply chain risk management responsibilities.

SA-02: ALLOCATION OF RESOURCES

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning;

b. Determine, document, and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process; and

c. Establish a discrete line item for information security and privacy in organizational programming and budgeting documentation.

AGENCY IMPLEMENTATION STANDARDS

Std.01 —The DFPS Commissioner or his/her designated representative(s) shall allocate resources for ongoing information security remediation, implementation, and compliance activities that reduce risk to a level acceptable to the The DFPS Commissioner. [Source: 1 TAC 202.20(2)]

SUPPLEMENTAL GUIDANCE

Resource allocation for information security and privacy includes funding for system and services acquisition, sustainment, and supply chain-related risks throughout the system development life cycle.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Secure System and Software Development Life Cycle Standard. **State:** 1 TAC 202.20(2); DIR Security Control Standards Catalog. **Federal**: OMB A-130; NIST SP 800-37, 800-160-1; FBI CJIS CSP v5.9.	PM-9, PS-8, SA-8, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and services acquisition policy; system and services acquisition procedures; system and services acquisition strategy and plans; procedures addressing the allocation of resources to information security and privacy requirements; procedures addressing capital planning and investment control; organizational programming and budgeting documentation; system security plan; privacy plan; supply chain risk management policy; other relevant documents or records.

Interview: Organizational personnel with capital planning, investment control, organizational programming, and budgeting responsibilities; organizational personnel with information security and privacy responsibilities; organizational personnel with supply chain risk management responsibilities.

Test: Organizational processes for determining information security and privacy requirements; organizational processes for capital planning, programming, and budgeting; automated mechanisms supporting and/or implementing organizational capital planning, programming, and budgeting.

SA-03: SYSTEM DEVELOPMENT LIFE CYCLE

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS, Privacy

CONTROL REQUIREMENTS

The organization:

a. Acquire, develop, and manage the system using DFPS's system development life cycle that incorporates information security and privacy considerations;

b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle;

c. Identify individuals having information security and privacy roles and responsibilities; and

d. Integrate the organizational information security and privacy risk management process into system development life cycle activities.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Information security, security testing, and audit controls shall be included in all phases of the system development lifecycle or acquisition process. [Source: DIR Control Standards Catalog SA-3]

Std.02 — The DFPS Commissioner or his/her designated representative(s) shall ensure that information security management processes are integrated with agency strategic and operational planning processes. [Source: 1 TAC 202.20(8)]

Std.03 — The DFPS Chief Information Security Officer shall be responsible for working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks. [Source: 1 TAC 202.21(b)(3)]

Std.04 — The DFPS Chief Information Security Officer shall be responsible for developing and recommending policies and establishing procedures and practices, in cooperation with the agency Information Resources Manager, information-owners and custodians, necessary to ensure the security of information and information

resources against unauthorized or accidental modification, destruction, or disclosure. [Source: 1 TAC 202.21(b)(8)]

SUPPLEMENTAL GUIDANCE

A system development life cycle process provides the foundation for the successful development, implementation, and operation of organizational systems. The integration of security and privacy considerations early in the system development life cycle is a foundational principle of systems security engineering and privacy engineering. To apply the required controls within the system development life cycle requires a basic understanding of information security and privacy, threats, vulnerabilities, adverse impacts, and risk to critical mission and business functions. The security engineering principles in SA-08 help individuals properly design, code, and test systems and system components. Organizations include qualified personnel (e.g., senior agency information security officers, senior agency officials for privacy, security and privacy architects, and security and privacy engineers) in system development life cycle processes to ensure that established security and privacy requirements are incorporated into organizational systems. Role-based security and privacy training programs can ensure that individuals with key security and privacy roles and responsibilities have the experience, skills, and expertise to conduct assigned system development life cycle activities.

The effective integration of security and privacy requirements into enterprise architecture also helps to ensure that important security and privacy considerations are addressed throughout the system life cycle and that those considerations are directly related to organizational mission and business processes. This process also facilitates the integration of the information security and privacy architectures into the enterprise architecture, consistent with the risk management strategy of the organization. Because the system development life cycle involves multiple organizations, (e.g., external suppliers, developers, integrators, service providers), acquisition and supply chain risk management functions and controls play significant roles in the effective management of the system during the life cycle.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Secure System and Software Development Life Cycle Standard. **State:** 1 TAC 202.20(8), 1 TAC 202.21(b)(3), 1 TAC 202.21(b)(8); TX Govt. Code 2054.112; DIR Security Control Standards Catalog. **Federal**: OMB A-130; NIST SP 800-30, 800-37, 800-160-1, 800-171, 800-172; FBI CJIS CSP v5.9	AT-3, PL-8, PM-7, SA-4, SA-5, SA-8, SA-11, SA-15, SA-17, SA-22, SR-3, SR-4, SR-5, SR-9.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and services acquisition policy; system and services acquisition procedures; procedures addressing the integration of information security and privacy and supply chain risk management into the system development life cycle process; system development life cycle documentation; organizational risk management strategy; information security and privacy risk management strategy documentation; system security plan; privacy plan; privacy program plan; enterprise architecture documentation; role-based security and privacy training program documentation; data mapping documentation; other relevant documents or records.

Interview: Organizational personnel with information security and privacy responsibilities; organizational personnel with system life cycle development responsibilities; organizational personnel with supply chain risk management responsibilities.

Test: Organizational processes for defining and documenting the system development life cycle; organizational processes for identifying system development life cycle roles and responsibilities; organizational processes for

integrating information security and privacy and supply chain risk management into the system development life cycle; automated mechanisms supporting and/or implementing the system development life cycle.

SA-03(02): USE OF LIVE OR OPERATIONAL DATA

Priority: P1

Baseline(s): Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization requires the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Require the developer of the system, system component, or system service to meet or exceed the baseline by security categorization provided in the DFPS Configuration Management Policy.

SUPPLEMENTAL GUIDANCE

Specifications for the security control requirements include that security controls be incorporated in the information system, supplemented by manual controls as needed. These considerations are applied when evaluating software packages, developed, or purchased.

Security requirements and controls reflect the business value of the information assets involved, and the potential business damage that might result from a failure or absence of security. [Source: Hitrust CSF 10.a Security Requirements Analysis and Specification]

Functional properties of security and privacy controls describe the functionality (i.e., security or privacy capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Configuration Management Policy; DFPS Secure System and Software Development Life Cycle Standard. **State:** DIR Security Control Standards Catalog. **Federal**: Privacy Act; OMB A-130; ISO 15408-1, 15408-2, 15408-3, 29148; FIPS 140, 201; NIST SP 800-35, 800-37, 800-70, 800-73-4, 800-137, 800-160-1, 800-161; NIST IR 7539; FBI CJIS CSP v5.9	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and services acquisition policy; system and services acquisition procedures; procedures addressing the integration of security and privacy requirements, descriptions, and criteria into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for the system, system component, or system services; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with acquisition/contracting responsibilities; organizational personnel with information security and privacy responsibilities; system developers.

Test: Organizational processes for determining system security functional requirements; organizational processes for developing acquisition contracts; automated mechanisms supporting and/or implementing acquisitions and the inclusion of security and privacy requirements in contracts.

SA-04: ACQUISITION PROCESS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS, Privacy

CONTROL REQUIREMENTS

The organization:

a. Include the following requirements, descriptions, and criteria, explicitly or by reference, using standardized contract language provided by the Information Technology and Security Requirements Attachment in the acquisition contract for the system, system component, or system service:

b. Security and privacy functional requirements;

c. Strength of mechanism requirements;

d. Security and privacy assurance requirements;

e. Controls needed to satisfy the security and privacy requirements.

f. Security and privacy documentation requirements;

g. Requirements for protecting security and privacy documentation;

h. Description of the system development environment and environment in which the system is intended to operate;

i. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and

j. Acceptance criteria.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS must include security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable laws and standards. [Source: DIR Control Standards Catalog SA-4]

Std.02 — The Information Security Officer shall be responsible for coordinating the review of data security requirements, specifications, and, if applicable, third-party risk assessment of any new computer applications or services that receive, maintain, and/or share confidential data. [Source: 1 TAC 202.21(b)(9)]

Std.03 — The DFPS Chief Information Security Officer shall be responsible for verifying that security requirements are identified and risk mitigation plans are developed and contractually agreed and obligated prior to the purchase of information technology hardware, software, and systems development services for any new high impact computer applications or computer applications that receive, maintain, and/or share confidential data. [Source: 1 TAC 202.21(b)(10)]

Std.04 — Where software development is outsourced, the following points are addressed either in a contract or security service level agreement (SLA):

a. Licensing arrangements, code ownership, and intellectual property rights;

b. Certification of the quality and accuracy of the work carried out;

c. Escrow arrangements in the event of failure of the third-party;

d. Rights of access for audit of the quality and accuracy of work done;

e. Contractual requirements for quality and security functionality of code; and

f. Testing before installation to detect malicious code. [Source: Hitrust 10.l Outsourced Software Development]

SUPPLEMENTAL GUIDANCE

Security and privacy functional requirements are typically derived from the high-level security and privacy requirements described in SA-02. The derived requirements include security and privacy capabilities, functions, and mechanisms. Strength requirements associated with such capabilities, functions, and mechanisms include degree of correctness, completeness, resistance to tampering or bypass, and resistance to direct attack. Assurance requirements include development processes, procedures, and methodologies as well as the evidence from development and assessment activities that provide grounds for confidence that the required functionality is implemented and possesses the required strength of mechanism. SP 800-160-1 describes the process of requirements engineering as part of the system development life cycle.

Controls can be viewed as descriptions of the safeguards and protection capabilities appropriate for achieving the particular security and privacy objectives of the organization and for reflecting the security and privacy requirements of stakeholders. Controls are selected and implemented in order to satisfy system requirements and include developer and organizational responsibilities. Controls can include technical, administrative, and physical aspects. In some cases, the selection and implementation of a control may necessitate additional specification by the organization in the form of derived requirements or instantiated control parameter values. The derived requirements and control parameter values may be necessary to provide the appropriate level of implementation detail for controls within the system development life cycle.

Security and privacy documentation requirements address all stages of the system development life cycle. Documentation provides user and administrator guidance for the implementation and operation of controls. The level of detail required in such documentation is based on the security categorization or classification level of the system and the degree to which organizations depend on the capabilities, functions, or mechanisms to meet risk response expectations. Requirements can include mandated configuration settings that specify allowed functions, ports, protocols, and services. Acceptance criteria for systems, system components, and system services are defined in the same manner as the criteria for any organizational acquisition or procurement.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Secure System and Software Development Life Cycle Standard. **State:** 1 TAC 202.21(b)(9), 1 TAC 202.21(b)(10); DIR Security Control Standards Catalog. **Federal**: Privacy Act; OMB A-130; ISO 15408-1, 15408-2, 15408-3, 29148; FIPS 140, 201; NIST SP 800-35, 800-37, 800-70, 800-73-4, 800-137, 800-160-1, 800-161; NIST IR 7539; 7622, 7676, 7870, 8062; NIAP Common Criteria Evaluation and Validation Scheme; NSA CSFC; FBI CJIS CSP v5.9.	CM-6, CM-8, PS-7, SA-3, SA-5, SA-8, SA-11, SA-15, SA-16, SA-17, SA-21, SR-3, SR-5.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and services acquisition policy; system and services acquisition procedures; procedures addressing the integration of information security and privacy and supply chain risk management into the acquisition process; configuration management plan; acquisition contracts for the system, system component, or system service; system design documentation; system security plan; supply chain risk management plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with acquisition/contracting responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators; organizational personnel with supply chain risk management responsibilities.

Test: Organizational processes for determining system security and privacy functional, strength, and assurance requirements; organizational processes for developing acquisition contracts; automated mechanisms supporting and/or implementing acquisitions and the inclusion of security and privacy requirements in contracts.

SA-04(01): FUNCTIONAL PROPERTIES OF SECURITY CONTROLS

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS, Privacy

CONTROL REQUIREMENTS

The organization requires the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Require the developer of the system, system component, or system service to meet or exceed the baseline by security categorization provided in the DFPS Configuration Management Policy.

SUPPLEMENTAL GUIDANCE

Specifications for the security control requirements include that security controls be incorporated in the information system, supplemented by manual controls as needed. These considerations are applied when evaluating software packages, developed, or purchased.

Security requirements and controls reflect the business value of the information assets involved, and the potential business damage that might result from a failure or absence of security. [Source: Hitrust CSF 10.a Security Requirements Analysis and Specification]

Functional properties of security and privacy controls describe the functionality (i.e., security or privacy capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Configuration Management Policy; DFPS Secure System and Software Development Life Cycle Standard. **State:** DIR Security Control Standards Catalog. **Federal**: Privacy Act; OMB A-130; ISO 15408-1, 15408-2, 15408-3, 29148; FIPS 140, 201; NIST SP 800-35, 800-37, 800-70, 800-73-4, 800-137, 800-160-1, 800-161; NIST IR 7539; FBI CJIS CSP v5.9	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and services acquisition policy; system and services acquisition procedures; procedures addressing the integration of security and privacy requirements, descriptions, and criteria into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for the system, system component, or system services; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with acquisition/contracting responsibilities; organizational personnel with information security and privacy responsibilities; system developers.

Test: Organizational processes for determining system security functional requirements; organizational processes for developing acquisition contracts; automated mechanisms supporting and/or implementing acquisitions and the inclusion of security and privacy requirements in contracts.

SA-04(02): DESIGN / IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS

Priority: P1

Baseline(s): Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes:

a. Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; and design and implementation information as specified in contracts or service level agreements (SLAs) at a level of detail sufficient to allow independent analysis.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Organizations may require different levels of detail in the documentation for the design and implementation of controls in organizational systems, system components, or system services based on mission and business requirements, requirements for resiliency and trustworthiness, and requirements for analysis and testing. Systems can be partitioned into multiple subsystems. Each subsystem within the system can contain one or more modules. The high-level design for the system is expressed in terms of subsystems and the interfaces between subsystems providing security-relevant functionality. The low-level design for the system is expressed in terms of modules and the interfaces between modules providing security-relevant functionality. Design and implementation documentation can include manufacturer, version, serial number, verification hash signature, software libraries used, date of purchase or download, and the vendor or download source. Source code and hardware schematics are referred to as the implementation representation of the system.

REFERENCES	RELATED CONTROLS

Agency: DFPS Information Security Policy; DFPS Configuration Management Policy; DFPS Secure System and Software Development Life Cycle Standard. **State:** DIR Security Control Standards Catalog. **Federal**: Privacy Act; OMB A-130; ISO 15408-1, 15408-2, 15408-3, 29148; FIPS 140, 201; NIST SP 800-35, 800-37, 800-70, 800-73-4, 800-137, 800-160-1, 800-161; NIST IR 7539; FBI CJIS CSP v5.9	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and services acquisition policy; system and services acquisition procedures; procedures addressing the integration of security requirements, descriptions, and criteria into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for the system, system components, or system services; design and implementation information for controls employed in the system, system component, or system service; system security plan; other relevant documents or records.

Interview: Organizational personnel with acquisition/contracting responsibilities; organizational personnel with the responsibility to determine system security requirements; system developers or service provider; organizational personnel with information security responsibilities.

Test: Organizational processes for determining the level of detail for system design and controls; organizational processes for developing acquisition contracts; automated mechanisms supporting and/or implementing development of system design details.

SA-04(09): FUNCTIONS / PORTS / PROTOCOLS / SERVICES IN USE

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization requires the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

The identification of functions, ports, protocols, and services early in the system development life cycle (e.g., during the initial requirements definition and design stages) allows organizations to influence the design of the system, system component, or system service. This early involvement in the system development life cycle helps organizations avoid or minimize the use of functions, ports, protocols, or services that pose unnecessarily high risks and understand the trade-offs involved in blocking specific ports, protocols, or services or requiring system service providers to do so. Early identification of functions, ports, protocols, and services avoids costly retrofitting of controls after the system, component, or system service has been implemented. SA-09 describes the requirements for external system services. Organizations identify which functions, ports, protocols, and services are provided from external sources.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Configuration Management Policy; DFPS Secure System and Software Development Life Cycle Standard. **State:** DIR Security Control Standards Catalog. **Federal**: Privacy Act; OMB A-130; ISO 15408-1, 15408-2, 15408-3, 29148; FIPS 140, 201; NIST SP 800-35, 800-37, 800-70, 800-73-4, 800-137, 800-160-1, 800-161; NIST IR 7539; FBI CJIS CSP v5.9	CM-7, SA-9.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and services acquisition policy; procedures addressing the integration of security requirements, descriptions, and criteria into the acquisition process; system design documentation; system documentation, including functions, ports, protocols, and services intended for organizational use; acquisition contracts for systems or services; acquisition documentation; solicitation documentation; service level agreements; organizational security requirements, descriptions, and criteria for developers of systems, system components, and system services; system security plan; other relevant documents or records.

Interview: Organizational personnel with acquisition/contracting responsibilities; organizational personnel with the responsibility for determining system security requirements; system/network administrators; organizational personnel operating, using, and/or maintaining the system; system developers; organizational personnel with information security responsibilities.

SA-05: INFORMATION SYSTEM DOCUMENTATION

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Obtain or develop administrator documentation for the system, system component, or system service that describes:
   1. Secure configuration, installation, and operation of the system, component, or service;
   2. Effective use and maintenance of security and privacy functions and mechanisms; and
   3. Known vulnerabilities regarding configuration and use of administrative or privileged functions;

b. Obtain or develop user documentation for the system, system component, or system service that describes:
   1. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms;
   2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and

3. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals;

c. Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and take actions defined in Std.02 in response; and

d. Distribute documentation to personnel identified in the System Security Plan (SSP).

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Obtain, protect as required, and make available to authorized personnel, adequate documentation for the information system. [Source: DIR Control Standards Catalog SA-5]

Std.02 — When documentation cannot be obtained, record in the System Security Plan (SSP):

a. The missing documentation types and topics as defined in this control; and

b. Auditable information, such as e-mails, meeting minutes, or other artifacts, regarding attempts to obtain documentation.

SUPPLEMENTAL GUIDANCE

System documentation helps personnel understand the implementation and operation of controls. Organizations consider establishing specific measures to determine the quality and completeness of the content provided. System documentation may be used to support the management of supply chain risk, incident response, and other functions. Personnel or roles that require documentation include system owners, system security officers, and system administrators. Attempts to obtain documentation include contacting manufacturers or suppliers and conducting web-based searches. The inability to obtain documentation may occur due to the age of the system or component or the lack of support from developers and contractors. When documentation cannot be obtained, organizations may need to recreate the documentation if it is essential to the implementation or operation of the controls. The protection provided for the documentation is commensurate with the security category or classification of the system. Documentation that addresses system vulnerabilities may require an increased level of protection. Secure operation of the system includes initially starting the system and resuming secure system operation after a lapse in system operation.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Configuration Management Policy; DFPS Secure System and Software Development Life Cycle Standard. **State:** DIR Security Control Standards Catalog. **Federal**: NIST SP 800-160-1; FBI CJIS CSP v5.9	CM-4, CM-6, CM-7, CM-8, PL-2, PL-4, PL-8, PS-2, SA-3, SA-4, SA-8, SA-9, SA-10, SA-11, SA-15, SA-16, SA-17, SI-12, SR-3.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; assessment report; vulnerability scanning tools and associated configuration documentation; vulnerability scanning results; patch and vulnerability management records; system security plan; other relevant documents or records.

Interview: Organizational personnel with risk assessment, control assessment, and vulnerability scanning responsibilities; organizational personnel with vulnerability scan analysis responsibilities; organizational

personnel with vulnerability remediation responsibilities; organizational personnel with security responsibilities; system/network administrators.

Test: Organizational processes for vulnerability scanning, analysis, remediation, and information sharing; automated mechanisms supporting and/or implementing vulnerability scanning, analysis, remediation, and information sharing

SA-08: SECURITY ENGINEERING PRINCIPLES

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization applies the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: systems security and privacy engineering principles in Std.01.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — System security and privacy engineering principles that must be applied are those principles defined in the DFPS SDLC, including at a minimum the following principles drafted according to the guidance in NIST SP 800-160-1:

a. Security Architecture and Design;

b. Security Capability and Intrinsic Behaviors; and

c. Life Cycle Security.

Std.02 — Provide role-specific training for all personnel in roles with responsibilities that contribute to secure development. Periodically review role-specific training and update it as needed. [Source: SSDF draft PO.2.2]

Std.03 — The following security engineering techniques help manage risks:

1. Anticipate the maximum possible ways that a product or service can be misused and abused in order to help identify how to protect the product or system from such uses. Address intended and unintended use scenarios in architecture and design;
2. Limit the number, size, and privilege levels of critical elements. Using criticality analysis will aid in determining which elements or functions are critical;
3. Use security mechanisms that help to reduce opportunities to exploit supply chain vulnerabilities, including, for example, encryption, access control, identity management, and malware or tampering discovery;
4. Design information system components and elements to be difficult to disable (e.g., tamper- proofing techniques) and, if disabled, trigger notification methods such as audit trails, tamper evidence, or alarms;
5. Design delivery mechanisms (e.g., downloads for software) to avoid unnecessary exposure or access to the supply chain infrastructure and the information systems/components traversing supply chain during delivery; and
6. Design relevant validation mechanisms to be used during implementation and operation. [Source: SP 800-161]
7. Ensure that when industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.

SUPPLEMENTAL GUIDANCE

Systems security and privacy engineering principles are closely related to and implemented throughout the system development life cycle (see SA-03). Organizations can apply systems security and privacy engineering principles to new systems under development or to systems undergoing upgrades. For existing systems, organizations apply systems security and privacy engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware components within those systems.

The application of systems security and privacy engineering principles helps organizations develop trustworthy, secure, and resilient systems and reduces the susceptibility to disruptions, hazards, threats, and the creation of privacy problems for individuals. Examples of system security engineering principles include developing layered protections; establishing security and privacy policies, architecture, and controls as the foundation for design and development; incorporating security and privacy requirements into the system development life cycle; delineating physical and logical security boundaries; ensuring that developers are trained on how to build secure software; tailoring controls to meet organizational needs; and performing threat modeling to identify use cases, threat agents, attack vectors and patterns, design patterns, and compensating controls needed to mitigate risk.

Organizations that apply systems security and privacy engineering concepts and principles can facilitate the development of trustworthy, secure systems, system components, and system services; reduce risk to acceptable levels; and make informed risk management decisions. System security engineering principles can also be used to protect against certain supply chain risks, including incorporating tamper-resistant hardware into a design.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Configuration Management Policy; DFPS Secure System and Software Development Life Cycle Standard. **State:** DIR Security Control Standards Catalog. **Federal**: Privacy Act; OMB A-130; FIPS 199, 200; NIST SP 800-37, 800-53A, 800-60-1, 800-60-2, 800-160-1; NIST IR 8062; FBI CJIS CSP v5.9	CM-4, CM-6, CM-7, CM-8, PL-2, PL-4, PL-8, PS-2, SA-3, SA-4, SA-8, SA-9, SA-10, SA-11, SA-15, SA-16, SA-17, SI-12, SR-3.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Risk assessment policy; security and privacy risk assessment reports; acquisitions documents; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with assessment and auditing responsibilities; system/network administrators; system developers; program managers; legal counsel; organizational personnel with security and privacy responsibilities.

Test: Organizational processes for assessments and audits; automated mechanisms/tools supporting and/or implementing assessments and auditing.

SA-08(33): MINIMIZATION

Priority: P1

Baseline(s): N/A	Overlay(s): Privacy

CONTROL REQUIREMENTS

The organization implements the privacy principle of minimization using processes as defined in Std.01.

AGENCY IMPLEMENTATION STANDARDS

Std.01 —

a. Identify the minimum elements of personally identifiable information (PII) that are relevant and necessary to accomplish the legally authorized purpose of collection;

b. Limit the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent; and

c. Conduct an initial evaluation of PII holdings; and review those holdings at least biennially to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose

SUPPLEMENTAL GUIDANCE

The minimum set of sensitive personal information (SPI) elements required to support a specific organization business process may be a subset of the SPI the organization is authorized to collect.

The principle of minimization states that organizations should only process personally identifiable information that is directly relevant and necessary to accomplish an authorized purpose and should only maintain personally identifiable information for as long as is necessary to accomplish the purpose. Organizations have processes in place, consistent with applicable laws and policies, to implement the principle of minimization.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Configuration Management Policy; DFPS Secure System and Software Development Life Cycle Standard. **State:** DIR Security Control Standards Catalog. **Federal**: Privacy Act; OMB A-130; FIPS 199, 200; NIST SP 800-37, 800-53A, 800-60-1, 800-60-2, 800-160-1; NIST IR 8062.	PE-8, PM-25, SC-42, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and services acquisition policy; system and services acquisition procedures; personally identifiable information processing policy; procedures addressing the minimization of personally identifiable information in system design; system design documentation; system configuration settings and associated documentation; change control records; information security and privacy requirements and specifications for the system; system security and privacy architecture; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records.

Interview: Organizational personnel with information security and privacy responsibilities; organizational personnel with system specification, design, development, implementation, and modification responsibilities; system developers.

Test: Organizational processes for applying the privacy design principle of minimization in system specification, design, development, implementation, and modification; automated mechanisms supporting the application of the security design principle of sufficient documentation in system specification, design, development,

implementation, and modification; automated mechanisms that enforce security and privacy policy; organizational processes for managing change configuration; automated mechanisms supporting configuration control.

SA-09: EXTERNAL INFORMATION SYSTEM SERVICES

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS, Privacy

CONTROL REQUIREMENTS

The organization:

a. Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: security and privacy controls as defined in DFPS Configuration Management Policy and service level agreements (SLAs);

b. Define and document organizational oversight and user roles and responsibilities with regard to external system services; and

c. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: processes, methods, and techniques as specified in contracts, SLAs, and the Continuous Monitoring Program (see CA-07).

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Ensure that SLAs include:

a. Service definitions;

b. Delivery levels;

c. Security controls, including third-party personnel security, information classification, transmission, and authorization;

d. Aspects of service management, including monitoring, auditing, impacts to the organization's resilience, and change management; and

e. Issues of liability, reliability of services and response times for the provision of services. [Source: Hitrust 09.e Service Delivery]

SUPPLEMENTAL GUIDANCE

External system services are provided by an external provider, and the organization has no direct control over the implementation of the required controls or the assessment of control effectiveness. Organizations establish relationships with external service providers in a variety of ways, including through business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, joint ventures, and supply chain exchanges. The responsibility for managing risks from the use of external system services remains with authorizing officials. For services external to organizations, a chain of trust requires that organizations establish and retain a certain level of confidence that each provider in the consumer-provider relationship provides adequate protection for the services rendered. The extent and nature of this chain of trust vary based on relationships between organizations and the external providers. Organizations document the basis for the trust relationships so that the relationships can be monitored. External system services documentation includes government, service providers, end user security roles and responsibilities, and service-level agreements. Service-level agreements define the expectations of performance for implemented controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; NIST SP 800-35, 800-160-1, 800-161, 800-171; NIST IR 8062.	AC-20, CA-3, CP-2, IR-4, IR-7, PL-10, PL-11, PS-7, SA-2, SA-4, SR-3, SR-5.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Organizational personnel with acquisition responsibilities; external providers of system services; organizational personnel with information security and privacy responsibilities; organizational personnel with supply chain risk management responsibilities.

Interview: Organizational processes for monitoring security and privacy control compliance by external service providers on an ongoing basis; automated mechanisms for monitoring security and privacy control compliance by external service providers on an ongoing basis.

SA-09(01): RISK ASSESSMENTS / ORGANIZATIONAL APPROVALS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization:

a. Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; and

b. Ensures that the acquisition or outsourcing of dedicated information security services is approved by the DFPS Chief Information Security Officer.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — The DFPS chief information officer must approve all acquisition or outsourcing of dedicated information security services based on the risk to the agency.

Std.02 — The DFPS Commissioner or his/her designated representative(s) must approve high level risk management decisions as required by 1 TAC 202. [Source: 1 TAC 202.20(6)]

SUPPLEMENTAL GUIDANCE

Dedicated information security services include, for example, incident monitoring, analysis and response, operation of information security-related devices such as firewalls, or key management services.

REFERENCES	RELATED CONTROLS

Agency: DFPS Information Security Policy; DFPS Secure System and Software Development Life Cycle Standard. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; NIST SP 800-35, 800-160-1, 800-161, 800-171; NIST IR 8062; FBI CJIS CSP v5.9.	CA-6, RA-3, RA-8.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and services acquisition policy; supply chain risk management policy and procedures; procedures addressing external system services; acquisition documentation; acquisition contracts for the system, system component, or system service; risk assessment reports; approval records for the acquisition or outsourcing of dedicated security services; system security plan; supply chain risk management plan; other relevant documents or records.

Interview: Organizational personnel with system and service acquisition responsibilities; organizational personnel with system security responsibilities; external providers of system services; organizational personnel with information security responsibilities; organizational personnel with supply chain risk management responsibilities.

Test: Organizational processes for conducting a risk assessment prior to acquiring or outsourcing dedicated security services; organizational processes for approving the outsourcing of dedicated security services; automated mechanisms supporting and/or implementing risk assessment; automated mechanisms supporting and/or implementing approval processes.

SA-09(02): IDENTIFICATION OF FUNCTIONS / PORTS / PROTOCOLS / SERVICES

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization requires providers of the following external system services to identify the functions, ports, protocols, and other services required for the use of such services: all external systems and services that have a dedicated connection with DFPS.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Ensure required functions, ports, protocols, and other services required for enabling the dedicated connection with DFPS are:

a. Authorized in accordance with CA-03;

b. Documented in the System Security Plan (SSP); and

c. Appropriately whitelisted or blacklisted in accordance with configuration management policy and procedures.

SUPPLEMENTAL GUIDANCE

Information from external service providers regarding the specific functions, ports, protocols, and services used in the provision of such services can be useful when the need arises to understand the trade-offs involved in restricting certain functions and services or blocking certain ports and protocols.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Secure System and Software Development Life Cycle Standard. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; NIST SP 800-35, 800-160-1, 800-161, 800-171; FBI CJIS CSP v5.9.	CM-6, CM-7.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and services acquisition policy; supply chain risk management policy and procedures; procedures addressing external system services; acquisition contracts for the system, system component, or system service; acquisition documentation; solicitation documentation; service level agreements; organizational security requirements and security specifications for external service providers; list of required functions, ports, protocols, and other services; system security plan; other relevant documents or records.

Interview: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; system/network administrators; external providers of system services.

SA-09(05): PROCESSING, STORAGE, AND SERVICE LOCATION

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization restricts the location of processing information and data system services to the Continental United States.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — For cloud based services, DFPS restricts the location of information processing, information/data, and information system services to the Continental United States. In no case may the safeguards afforded to sensitive information be less than the safeguards mandates by the FBI CJIS Security Policy, federal law, Executive Order, or other authoritative direction.

SUPPLEMENTAL GUIDANCE

Information from external service providers regarding the specific functions, ports, protocols, and services used in the provision of such services can be useful when the need arises to understand the trade-offs involved in restricting certain functions and services or blocking certain ports and protocols.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; NIST SP 800-35, 800-160-1, 800-161, 800-171; FBI CJIS CSP v5.9.	SA-5, SR-4.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and services acquisition policy; procedures addressing external system services; acquisition contracts for the system, system component, or system service; solicitation documentation; acquisition documentation; service level agreements; restricted locations for information processing; information/data and/or system services; information processing, information/data, and/or system services to be maintained in restricted locations; organizational security requirements or conditions for external providers; system security plan; supply chain risk management plan; other relevant documents or records.

Interview: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; external providers of system services; organizational personnel with supply chain risk management responsibilities.

Test: Organizational processes for defining the requirements to restrict locations of information processing, information/data, or information services; organizational processes for ensuring the location is restricted in accordance with requirements or conditions.

SA-10: DEVELOPER CONFIGURATION MANAGEMENT

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization requires the developer of the information system, system component, or information system service to:

a. Perform configuration management during system, component, or service design, development, implementation, operation, and disposal;

b. Document, manage, and control the integrity of changes to all configuration items under configuration management;

c. Implement only organization-approved changes to the system, component, or service;

d. Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes; and

e. Track security flaws and flaw resolution within the system, component, or service and report findings to personnel identified in the System Security Plan (SSP).

AGENCY IMPLEMENTATION STANDARDS

Std.01 — All security-related information resources changes shall be approved by the information owner through a change control process (i.e. CAB Approval). Approval shall occur prior to implementation by DFPS or independent contractors. [Source: DIR Control Standards Catalog SA-10]

SUPPLEMENTAL GUIDANCE

Organizations consider the quality and completeness of configuration management activities conducted by developers as direct evidence of applying effective security controls. Controls include protecting the master copies of material used to generate security-relevant portions of the system hardware, software, and firmware from unauthorized modification or destruction. Maintaining the integrity of changes to the system, system component, or system service requires strict configuration control throughout the system development life cycle to track authorized changes and prevent unauthorized changes.

The configuration items that are placed under configuration management include the formal model; the functional, high-level, and low-level design specifications; other design data; implementation documentation; source code and hardware schematics; the current running version of the object code; tools for comparing new versions of security-relevant hardware descriptions and source code with previous versions; and test fixtures and documentation. Depending on the mission and business needs of organizations and the nature of the contractual relationships in place, developers may provide configuration management support during the operations and maintenance stage of the system development life cycle.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy; DFPS Secure System and Software Development Life Cycle Standard. **State:** DIR Security Control Standards Catalog. **Federal**: FIPS 140, 180, 202; NIST SP 800-128, 800-160-1; FBI CJIS CSP v5.9.	CM-2, CM-3, CM-4, CM-7, CM-9, SA-4, SA-5, SA-8, SA-15, SI-2, SR-3, SR-4, SR-5, SR-6.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and services acquisition policy; procedures addressing system developer configuration management; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; system developer configuration management plan; security flaw and flaw resolution tracking records; system change authorization records; change control records; configuration management records; system security plan; other relevant documents or records.

Interview: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with configuration management responsibilities; system developers.

Test: Organizational processes for monitoring developer configuration management; automated mechanisms supporting and/or implementing the monitoring of developer configuration management.

SA-11: DEVELOPER SECURITY TESTING AND EVALUATION

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS, Privacy

CONTROL REQUIREMENTS

The organization requires the developer of the information system, system component, or information system service to:

a. Develop and implement a plan for ongoing security and privacy control assessments;
b. Perform unit, integration, system, and regression testing/evaluation as specified in Std.01 at an organization-defined depth and coverage to include, at a minimum, the system components to be scanned and the vulnerabilities to be checked;
c. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation;
d. Implement a verifiable flaw remediation process; and
e. Correct flaws identified during testing and evaluation.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Perform testing at frequencies:

a. In accordance with the organization's defined System Development Life Cycle (SDLC);
b. Before being placed in the production environment; and
c. Whenever security-relevant modifications have been made to the information system subsequent to developer testing.

Std.02 — Include contractual language requiring developers of systems, components, or solutions to create and document security testing plans and test all required security controls.

Std.03 — Require developers to document and approve test plans that define responsibilities for parties involved and a comprehensive set of test transactions and test data that represents the various activities and conditions that will be encountered in processing.

Std.04 — For all moderate- or high-impact systems under development, ensure security test results are required elements in the acceptance criteria for the system.

Std.05 — For all moderate- or high-impact systems, ensure security test results are considered during the authorization to operate process (ATO).

SUPPLEMENTAL GUIDANCE

Developmental security testing/evaluation occurs at all post-design phases of the system development life cycle. Such testing/evaluation confirms that the required security controls are implemented correctly, operating as intended, enforcing the desired security policy, and meeting established security requirements. Security properties of information systems may be affected by the interconnection of system components or changes to those components. These interconnections or changes (e.g., upgrading or replacing applications and operating systems) may adversely affect previously implemented security controls. This control provides additional types of security testing/evaluation that developers can conduct to reduce or eliminate potential flaws. Testing custom software applications may require approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches.

Developers can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Security assessment plans provide the specific activities that developers plan to carry out including the types of analyses, testing, evaluation, and reviews of software and firmware components, the degree of rigor to be applied, and the types of artifacts produced during those processes. The depth of security testing/evaluation refers to the rigor and level of detail associated with the assessment process (e.g., black box, gray box, or white box testing). The coverage of security testing/evaluation refers to the scope (i.e., number and type) of the artifacts included in the assessment process. Contracts specify the acceptance criteria for security assessment plans, flaw remediation processes, and the evidence that the plans/processes have been diligently applied. Methods for reviewing and protecting

assessment plans, evidence, and documentation are commensurate with the security category or classification level of the information system. Contracts may specify documentation protection requirements.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; DFPS Secure System and Software Development Life Cycle Standard. **State:** TX Govt. Code 2054.516; DIR Security Control Standards Catalog. **Federal**: ISO 15408-3; NIST SP 800-30, 800-53A, 800-154, 800-160-1; FBI CJIS CSP v5.9.	CA-2, CA-7, CM-4, SA-3, SA-4, SA-5, SA-8, SA-15, SA-17, SI-2, SR-5, SR-6, SR-7.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and services acquisition policy; system and services acquisition procedures; procedures addressing system developer security and privacy testing; procedures addressing flaw remediation; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; security and privacy architecture; system design documentation; system developer security and privacy assessment plans; results of developer security and privacy assessments for the system, system component, or system service; security and privacy flaw and remediation tracking records; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records.

Interview: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security and privacy responsibilities; organizational personnel with developer security and privacy testing responsibilities; system developers.

Test: Organizational processes for monitoring developer security testing and evaluation; automated mechanisms supporting and/or implementing the monitoring of developer security and privacy testing and evaluation.

SA-11(01): STATIC CODE ANALYSIS

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization requires the developer of the information system, system component, or information system service to employ static code analysis tools to identify common flaws and document the results of the analysis.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Static code analysis must be a design requirement for all system, system component, or system service projects developed on behalf of the organization.

Std.02 — Require the developer to use only approved tools and libraries for static code analysis, and to address vulnerabilities discovered through use of those tools and libraries.

Std.03 — Require the developer to perform static code analysis in accordance with the organization's Software Development Life Cycle (SDLC).

SUPPLEMENTAL GUIDANCE

Static code analysis provides a technology and methodology for security reviews and includes checking for weaknesses in the code as well as for the incorporation of libraries or other included code with known vulnerabilities or that are out-of-date and not supported.

Static code analysis can be used to identify vulnerabilities and enforce secure coding practices. It is most effective when used early in the development process, when each code change can automatically be scanned for potential weaknesses. Static code analysis can provide clear remediation guidance and identify defects for developers to fix. Evidence of the correct implementation of static analysis can include aggregate defect density for critical defect types, evidence that defects were inspected by developers or security professionals, and evidence that defects were remediated. A high density of ignored findings, commonly referred to as false positives, indicates a potential problem with the analysis process or the analysis tool. In such cases, organizations weigh the validity of the evidence against evidence from other sources.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** TX Govt. Code 2054.516; DIR Security Control Standards Catalog. **Federal**: ISO 15408-3; NIST SP 800-30, 800-53A, 800-154, 800-160-1; FBI CJIS CSP v5.9.	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and services acquisition policy; system and services acquisition procedures; procedures addressing system developer security testing; procedures addressing flaw remediation; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; security and privacy architecture; system design documentation; system developer security and privacy assessment plans; results of system developer security and privacy assessments; security flaw and remediation tracking records; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records.

Interview: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with developer security and privacy testing responsibilities; organizational personnel with configuration management responsibilities; system developers.

Test: Organizational processes for monitoring developer security testing and evaluation; automated mechanisms supporting and/or implementing the monitoring of developer security testing and evaluation; static code analysis tools.

SA-11(02): THREAT AND VULNERABILITY ANALYSIS

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization requires the developer of the system, system component, or system service to perform threat modeling and vulnerability analyses during development and the subsequent testing and evaluation of the system, component, or service that:

a. Uses the following contextual information: information from system categorization, risk assessment, vulnerability scans, risk register, and/or authority to operate (ATO);

b. Employs the following tools and methods: tools and methods equivalent to or more thorough than scans performed by the Department of Information Resources (DIR);

c. Conducts the modeling and analyses at the following level of rigor: at organization-defined depth and coverage to include, at a minimum, the system components to be scanned and the vulnerabilities checked; and

d. Produces evidence that meets the following acceptance criteria: requirements of controls including CA-02, and any applicable service level agreements (SLAs).

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS, when implementing an Internet website or mobile application that processes any sensitive personal or personally identifiable information or confidential information must subject the website or application to a vulnerability and penetration test and address any vulnerability identified in the test. [Source: TX Govt. Code 2054.516(a)(2)]

Std.02 — The developer of the system, system component, must perform threat and vulnerabilities analyses and subsequent testing/evaluation of the as-built system, component, or service.

SUPPLEMENTAL GUIDANCE

Applications may deviate significantly from the functional and design specifications created during the requirements and design phases of the system development life cycle. Therefore, threat and vulnerability analyses of information systems, system components, and information system services prior to delivery are critical to the effective operation of those systems, components, and services. Threat and vulnerability analyses at this phase of the life cycle help to ensure that design or implementation changes have been accounted for, and that any new vulnerabilities created as a result of those changes have been reviewed and mitigated.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** TX Govt. Code 2054.516; DIR Security Control Standards Catalog. **Federal**: ISO 15408-3; NIST SP 800-30, 800-53A, 800-154, 800-160-1.	PM-15, RA-3, RA-5.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and services acquisition policy; procedures addressing system developer security testing; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; system developer security test plans; records of developer security testing results for the system, system component, or system service; vulnerability scanning results; system risk assessment reports; threat and vulnerability analysis reports; system security plan; supply chain risk management plan; other relevant documents or records.

Interview: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with developer security testing responsibilities; system developers; organizational personnel with supply chain risk management responsibilities.

Test: Organizational processes for monitoring developer security testing and evaluation; automated mechanisms supporting and/or implementing the monitoring of developer security testing and evaluation.

SA-11(05): PENETRATION TESTING

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization requires the developer of the system, system component, or system service to perform penetration testing:

a. At the following level of rigor: organization-defined breadth and depth to include, at a minimum, the system components to be scanned and the vulnerabilities checked; and

b. Under the following constraints: constraints defined in Stds.01 & 02

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS, when implementing an Internet website or mobile application that processes any sensitive personal or personally identifiable information or confidential information must subject the website or application to a vulnerability and penetration test and address any vulnerability identified in the test. [Source: TX Govt. Code 2054.516(a)(2)]

Std.02 — Require advanced coordination and formal authorization for all penetration testing on systems in the production environment. Authorization must include scope of test including, but not limited to, system components and planned actions.

SUPPLEMENTAL GUIDANCE

Reporting on penetration testing should include the defined list of targets provided (IP addresses, protocols, services, or applications, etc.); the specific commercial, public, and proprietary tools used; and, if applicable, evidence of successful exploitation or illustrations of exploitability where vulnerabilities exist.

Penetration testing is an assessment methodology in which assessors, using all available information technology product or system documentation and working under specific constraints, attempt to circumvent the implemented security and privacy features of information technology products and systems. Useful information for assessors who conduct penetration testing includes product and system design specifications, source code, and administrator and operator manuals. Penetration testing can include white-box, gray-box, or black-box testing with analyses performed by skilled professionals who simulate adversary actions. The objective of penetration testing is to discover vulnerabilities in systems, system components, and services that result from implementation errors, configuration faults, or other operational weaknesses or deficiencies. Penetration tests can be performed in conjunction with automated and manual code reviews to provide a greater level of analysis

than would ordinarily be possible. When user session information and other personally identifiable information is captured or recorded during penetration testing, such information is handled appropriately to protect privacy.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** TX Govt. Code 2054.516; DIR Security Control Standards Catalog. **Federal**: ISO 15408-3; NIST SP 800-30, 800-53A, 800-154, 800-160-1.	CA-8, PM-14, PM-25, PT-2, SA-3, SI-2, SI-6.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and services acquisition policy; system and services acquisition procedures; procedures addressing system developer security testing; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; system developer penetration testing and evaluation plans; system developer penetration testing and evaluation results; system security plan; privacy plan; personally identifiable information processing policy; other relevant documents or records.

Interview: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security and privacy responsibilities; organizational personnel with developer security testing responsibilities; system developers; independent verification agent.

Test: Organizational processes for monitoring developer security and privacy assessments; automated mechanisms supporting and/or implementing the monitoring of developer security and privacy assessments.

SA-11(08): DYNAMIC CODE ANALYSIS

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization requires the developer of the system, system component, or system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS, when implementing an Internet website or mobile application that processes any sensitive personal or personally identifiable information or confidential information, must subject the website or application to a vulnerability and penetration test and address any vulnerability identified in the test. [Source: TX Govt. Code 2054.516(a)(2)]

Std.02 — A security test and evaluation plan, including the use of dynamic code analysis at run-time, must be created and implemented for any information system developed on behalf of DFPS.

SUPPLEMENTAL GUIDANCE
Dynamic code analysis provides runtime verification of software programs using tools capable of monitoring programs for memory corruption, user privilege issues, and other potential security problems. Dynamic code analysis employs runtime tools to ensure that security functionality performs in the way it was designed. A type of dynamic analysis, known as fuzz testing, induces program failures by deliberately introducing malformed or random data into software programs. Fuzz testing strategies are derived from the intended use of applications and the functional and design specifications for the applications. To understand the scope of dynamic code analysis and the assurance provided, organizations may also consider conducting code coverage analysis (i.e., checking the degree to which the code has been tested using metrics such as percent of subroutines tested or percent of program statements called during execution of the test suite) and/or concordance analysis (i.e., checking for words that are out of place in software code, such as non-English language words or derogatory terms).

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** TX Govt. Code 2054.516; DIR Security Control Standards Catalog. **Federal**: ISO 15408-3; NIST SP 800-30, 800-53A, 800-154, 800-160-1.	N/A

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: System and services acquisition policy; procedures addressing system developer security testing; procedures addressing flaw remediation; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; system developer security test and evaluation plans; security test and evaluation results; security flaw and remediation tracking reports; system security plan; other relevant documents or records. Interview: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with developer security testing responsibilities; organizational personnel with configuration management responsibilities; system developers. Test: Organizational processes for monitoring developer security testing and evaluation; automated mechanisms supporting and/or implementing the monitoring of developer security testing and evaluation.

SA-12: SUPPLY CHAIN PROTECTION

Priority: P1	
Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS
This control is withdrawn and incorporated into SR Family but still referenced in the FBI CJIS Security Policy v5.9. Please see the SR Family of controls.

SA-12(01): ACQUISITION STRATEGIES / TOOLS / METHOD

Priority: P1	
Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

This control is withdrawn and incorporated into SR-06 but still referenced in the FBI CJIS Security Policy v5.9. Please see the SR-06.

SA-15: DEVELOPMENT PROCESS, STANDARDS, AND TOOLS

Priority: P1	
Baseline(s): High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization requires the developer of the system, system component, or system service to follow:

a. A documented development process that:
   1. Explicitly addresses security and privacy requirements;
   2. Identifies the standards and tools used in the development process;
   3. Documents the specific tool options and tool configurations used in the development process; and
   4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and

b. Review the development process, standards, tools, tool options, and tool configurations at least annually to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy the following security and privacy requirements: all applicable security and privacy requirements as identified in the System Security Plan (SSP).

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Developers must follow processes identified in the DFPS SDLC, which incorporates information security and privacy requirements.

Std.02 — SDLC processes must include provisions for documenting tool options and tool configurations.

Std.03 — Changes to tools and tool configurations in the DFPS environment must be managed in accordance with CM-03.

Std.04 — Developers must self-assess and attest, or permit DFPS to assess, the developer's process, standards, tools, and tool options/configurations as part of the source selection evaluation to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy all privacy and security requirements.

SUPPLEMENTAL GUIDANCE

Specifications for the security control requirements include that security controls be incorporated in the information system, supplemented by manual controls as needed. These considerations are applied when evaluating software packages, developed, or purchased.

Security requirements and controls reflect the business value of the information assets involved, and the potential business damage that might result from a failure or absence of security. For purchased commercial products, a formal acquisition process is followed.

Contracts with the supplier include the identified security requirements. Where the security functionality in a proposed product does not satisfy the specified requirement, then the risk introduced and associated controls are reconsidered prior to purchasing the product. Where additional functionality is supplied, and causes a security risk, this is disabled or mitigated through application of additional controls. The organization requires developers of information systems, components, and services to identify (document) early in the system development life cycle, the functions ports, protocols, and services intended for organizational use. [Source: Hitrust CSF 10.a Security Requirements Analysis and Specification]

Development tools include programming languages and computer-aided design systems. Reviews of development processes include the use of maturity models to determine the potential effectiveness of such processes. Maintaining the integrity of changes to tools and processes facilitates effective supply chain risk assessment and mitigation. Such integrity requires configuration control throughout the system development life cycle to track authorized changes and prevent unauthorized changes.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: NIST SP 800-160-1; NIST IR 8179.	MA-6, SA-3, SA-4, SA-8, SA-10, SA-11, SR-3, SR-4, SR-5, SR-6, SR-9.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and services acquisition policy; system and services acquisition procedures; procedures addressing development process, standards, and tools; procedures addressing the integration of security and privacy requirements during the development process; solicitation documentation; acquisition documentation; critical component inventory documentation; service level agreements; acquisition contracts for the system, system component, or system service; system developer documentation listing tool options/configuration guides; configuration management policy; configuration management records; documentation of development process reviews using maturity models; change control records; configuration control records; documented reviews of the development process, standards, tools, and tool options/configurations; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records.

Interview: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security and privacy responsibilities; system developer.

SA-16: DEVELOPER-PROVIDED TRAINING

Priority: P1

Baseline(s): High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization the developer of the system, system component, or system service to provide the following training on the correct use and operation of the implemented security and privacy functions, controls, and/or mechanisms: training defined in Std.01.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Require that training be provided as defined in Statements of Work (SOWs), to include, at a minimum, one of the following:

a. Role-based training for users, privileged users, admins, developers, security personnel, and others as specified (for example, trainers, support staff); or

b. Sufficient training materials for the organization to conduct in-house training or offer self- training to organizational personnel after initial system deployment.

SUPPLEMENTAL GUIDANCE

Agencies may contract with external vendors to provide qualified instructors and necessary instruction material, as agreed, to train personnel (including contractors and partners as applicable) in the secure and cost-effective use of products or services. Training content must address all stages from installation through decommissioning and known inherent risks and mitigations as appropriate to audience.

Developer-provided training applies to external and internal (in-house) developers. Training personnel is essential to ensuring the effectiveness of the controls implemented within organizational systems. Types of training include web-based and computer-based training, classroom-style training, and hands-on training (including micro-training). Organizations can also request training materials from developers to conduct in-house training or offer self- training to organizational personnel. Organizations determine the type of training necessary and may require different types of training for different security and privacy functions, controls, and mechanisms.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: None.	AT-2, AT-3, PE-3, SA-4, SA-5.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and services acquisition policy; system and services acquisition procedures; procedures addressing developer-provided training; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; organizational security and privacy training policy; developer-provided training materials; training records; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records.

Interview: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security and privacy responsibilities; system developer; external or internal (in-house) developers with training responsibilities for the system, system component, or information system service.

SA-17: DEVELOPER SECURITY ARCHITECTURE AND DESIGN

Priority: P1

Baseline(s): High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization the developer of the system, system component, or system service to produce a design specification and security and privacy architecture that:

a. Is consistent with the organization's security and privacy architecture that is an integral part the organization's enterprise architecture;

b. Accurately and completely describes the required security and privacy functionality, and the allocation of controls among physical and logical components; and

c. Expresses how individual security and privacy functions, mechanisms, and services work together to provide required security and privacy capabilities and a unified approach to protection.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Ensure developers produce design specifications and security architectures consistent with the agency's security architecture as defined in PL-08 and enterprise architecture as defined in PM-07.

Std.02 — Statements of business requirements for new information systems (developed or purchased), or enhancements to existing information systems shall specify the requirements for security and privacy controls. [Source: Hitrust 10.a Security Requirements Analysis and Specification]

SUPPLEMENTAL GUIDANCE

Developer security and privacy architecture and design are directed at external developers, although they could also be applied to internal (in-house) development. In contrast, PL-08 is directed at internal developers to ensure that organizations develop a security and privacy architecture that is integrated with the enterprise architecture. The distinction between SA- 17 and PL-08 is especially important when organizations outsource the development of systems, system components, or system services and when there is a requirement to demonstrate consistency with the enterprise architecture and security and privacy architecture of the organization. ISO 15408-2, ISO 15408-3, and SP 800-160-1 provide information on security architecture and design, including formal policy models, security- relevant components, formal and informal correspondence, conceptually simple design, and structuring for least privilege and testing.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: ISO 15408-2, 15408-3; NIST SP 800-160-1.	PL-2, PL-8, PM-7, SA-3, SA-4, SA-8, SC-7.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and services acquisition policy; system and services acquisition procedures; enterprise architecture policy; enterprise architecture documentation; procedures addressing developer security and privacy architecture and design specifications for the system; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; system design documentation; information system configuration settings and associated documentation; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with acquisition responsibilities; organizational personnel with information security and privacy responsibilities; system developer.

SA-21: DEVELOPER SCREENING

Priority: P1

Baseline(s): High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization information systems, system components, or information system services:

a. Have appropriate access authorizations as determined by assigned duties; and
b. Satisfy personnel screening criteria as defined by DFPS.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Ensure that the registration process to receive an account complies with requirements as defined in the DFPS Account Management Policy.

Std.02 — DFPS employees, as well as to many DFPS volunteers, interns, contractors, and employees of other state agencies are required to complete a Federal Bureau of Investigations (FBI) fingerprint check to access DFPS information resources. [Source: DFPS Background Checks Handbook]

SUPPLEMENTAL GUIDANCE

Because the information system, system component, or information system service may be employed in critical activities essential to the national and/or economic security interests of the United States, organizations have a strong interest in ensuring that the developer is trustworthy. The degree of trust required of the developer may need to be consistent with that of the individuals accessing the information system/component/service once deployed. Examples of authorization and personnel screening criteria include clearance, satisfactory background checks, citizenship, and nationality. Trustworthiness of developers may also include a review and analysis of company ownership and any relationships the company has with entities potentially affecting the quality/reliability of the systems, components, or services being developed.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: ISO 15408-2, 15408-3; NIST SP 800-160-1.	PS-2, PS-3, PS-6, PS-7, SA-4, SR-6.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and services acquisition policy; personnel security policy and procedures; procedures addressing personnel screening; system design documentation; acquisition documentation; service level agreements; acquisition contracts for developer services; system configuration settings and associated documentation; list of appropriate access authorizations required by the developers of the system; personnel screening criteria and associated documentation; system security plan; supply chain risk management plan; other relevant documents or records.

Interview: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel responsible for developer screening].

Test: Organizational processes for developer screening; automated mechanisms supporting developer screening.

SA-22: UNSUPPORTED SYSTEM COMPONENTS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization:

a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or

b. Provide the following options for alternative sources for continued support for unsupported components in-house support or support from external providers as specified in Statements of Work (SOWs).

AGENCY IMPLEMENTATION STANDARDS

Std.01 —

a. The Texas Department of Information Resources (DIR) shall conduct a study to identify legacy systems currently maintained by state agencies other than institutions of higher education. The study must include:
   1. An inventory of the systems maintained by state agencies;
   2. The annual cost and availability of resources to maintain the systems;
   3. The security risks related to use of the systems;
   4. If feasible, a cost estimate for updating the systems; and
   5. A plan for assessing and prioritizing statewide modernization projects to update or replace the systems.

b. The department may contract with a private vendor to conduct the study.

c. On request by the department, each state agency shall provide to the department the information necessary for the study. The department may require a state agency to clarify or validate information provided by the agency or related to the study. [Source: TX Govt. Code 2054.552(a, b, c)]

Std.02 — The exception process must be followed for any unsupported components in the DFPS environment of operations.

Std.03 — The support status of components must be documented in the System Security Plan (SSP) and system/component inventory.

Std.04 — If systems or system components in production are no longer supported by the developer, vendor, or manufacturer, the organization must show evidence of a formal migration plan approved by management to

replace the system or system component. [Source: Hitrust CSF 10.h Control of Operational Software] If replacement is not feasible, a mitigation plan must be developed.

SUPPLEMENTAL GUIDANCE

Texas Government Code provides the following definition: a "legacy system" means a computer system or application program that is operated with obsolete or inefficient hardware or software technology. [Source: TX Govt. Code 2054.551]

Support for system components includes software patches, firmware updates, replacement parts, and maintenance contracts. An example of unsupported components includes when vendors no longer provide critical software patches or product updates, which can result in an opportunity for adversaries to exploit weaknesses in the installed components.

Exceptions to replacing unsupported system components include systems that provide critical mission or business capabilities where newer technologies are not available or where the systems are so isolated that installing replacement components is not an option.

Alternative sources for support address the need to provide continued support for system components that are no longer supported by the original manufacturers, developers, or vendors when such components remain essential to organizational mission and business functions. If necessary, organizations can establish in-house support by developing customized patches for critical software components or, alternatively, obtain the services of external providers who provide ongoing support for the designated unsupported components through contractual relationships. Such contractual relationships can include open-source software value-added vendors. The increased risk of using unsupported system components can be mitigated, for example, by prohibiting the connection of such components to public or uncontrolled networks or implementing other forms of isolation.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** TX Govt. Code 2054; DIR Security Control Standards Catalog. **Federal**: ISO 15408-2, 15408-3; NIST SP 800-160-1.	PS-2, PS-3, PS-6, PS-7, SA-4, SR-6.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and services acquisition policy; personnel security policy and procedures; procedures addressing personnel screening; system design documentation; acquisition documentation; service level agreements; acquisition contracts for developer services; system configuration settings and associated documentation; list of appropriate access authorizations required by the developers of the system; personnel screening criteria and associated documentation; system security plan; supply chain risk management plan; other relevant documents or records.

Interview: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel responsible for developer screening].

Test: Organizational processes for developer screening; automated mechanisms supporting developer screening.

(SC) SYSTEM AND COMMUNICATIONS PROTECTION

DFPS requires the monitoring, control, and protection of DFPS communications (information transmitted or received by DFPS information systems). The SC control family is responsible for systems and communications protection procedures. This includes boundary protection, protection of information at rest, collaborative computing devices, cryptographic protection, denial of service protection, and many others.

The intended audience for this Control includes, but is not limited to, information resource owners and custodians. The information resource owner, or their designee, is responsible for ensuring that system and communication protection measures described in this Control family are implemented by personnel with risk management responsibilities (e.g. system/network administrators, information security analyst, etc.).

SC-01: SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Develop, document, and disseminate to appropriate personnel:
   1. Organization-level system and communications protection policy that:
      a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls;

b. Designate a senior management official as defined in the system and communications protection policy to manage the development, documentation, and dissemination of the system and communications protection policy and procedures; and

c. Review and update the current system and communications protection:
   1. Policy every year and following major changes to legislation or security requirements; and
   2. Procedures every year and following major changes to legislation or security requirements.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS must develop, disseminate, and periodically review/update:

a. A formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls. [Source: DIR Control Standards Catalog SC-1]

Std.02 — The DFPS Chief Information Security Officer shall be responsible for:

a. Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks;

b. Providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities under 1 TAC 202; and

c. Developing and recommending policies and establishing procedures and practices, in cooperation with the agency Information Resources Manager, information-owners and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, or disclosure. [Source: 1 TAC 202.21(b)(3, 5, 8)]

SUPPLEMENTAL GUIDANCE

System and communications protection policy and procedures address the controls in the SC family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of system and communications protection policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to system and communications protection policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** 1 TAC 202.22(1, 2); DIR Security Control Standards Catalog. **Federal**: OMB A-130; NIST SP 800-12, 800-100; FBI CJIS CSP v5.9.	PM-9, PS-8, SA-8, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; system and communications protection procedures; system security plan; privacy plan; risk management strategy documentation; audit findings; other relevant documents or records.

Interview: Organizational personnel with system and communications protection responsibilities; organizational personnel with information security and privacy responsibilities.

SC-02: SEPARATION OF SYSTEM AND USER FUNCTIONALITY

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The information system separates user functionality (including user interface services) from information system management functionality.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Design and configure systems to physically or logically separate user functionality from information storage and from management and administrative functionality, and to prevent users from performing any functions that are not explicitly authorized for their roles. Ensure that the functionality of one process or service given to one application does not enable the same functionality for another application.

SUPPLEMENTAL GUIDANCE

Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from information system management functionality is either physical or logical. Organizations implement separation of system management-related functionality from user functionality by using different computers, different central processing units, different instances of operating systems, different network addresses, virtualization techniques, or combinations of these or other methods, as appropriate. This type of separation includes, for example, web administrative interfaces that use separate authentication methods for users of any other information system resources. Separation of system and user functionality may include isolating administrative interfaces on different domains and with additional access controls.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** 1 TAC 202.22(1, 2); DIR Security Control Standards Catalog. **Federal**: FBI CJIS CSP v5.9.	AC-6, SA-4, SA-8, SC-3, SC-7, SC-22, SC-32, SC-39.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing application partitioning; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; system developer.

Test: Separation of user functionality from system management functionality.

SC-02(01): INTERFACES FOR NON-PRIVILEGED USERS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The information system separates user functionality (including user interface services) from information system management functionality.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Design and configure systems to physically or logically separate user functionality from information storage and from management and administrative functionality, and to prevent users from performing any functions that are not explicitly authorized for their roles. Ensure that the functionality of one process or service given to one application does not enable the same functionality for another application.

SUPPLEMENTAL GUIDANCE

Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from information system management functionality is either physical or logical. Organizations implement separation of system management-related functionality from user functionality by using different computers, different central processing units, different instances of operating systems, different network addresses, virtualization techniques, or combinations of these or other methods, as appropriate. This type of separation includes, for example, web administrative interfaces that use separate authentication methods for users of any other information system resources. Separation of system and user functionality may include isolating administrative interfaces on different domains and with additional access controls.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** 1 TAC 202.22(1, 2); DIR Security Control Standards Catalog. **Federal**: FBI CJIS CSP v5.9.	AC-6, SA-4, SA-8, SC-3, SC-7, SC-22, SC-32, SC-39.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing application partitioning; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; non-privileged users of the system; system developer.

Test: Separation of user functionality from system management functionality.

SC-03: SECURITY FUNCTION ISOLATION

Priority: P1

Baseline(s): High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The information system isolates security functions from non-security functions.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

The information system isolates security functions from non-security functions by means of an isolation boundary (implemented via partitions and domains). Such isolation controls access to and protects the integrity of the hardware, software, and firmware that perform those security functions. Information systems implement code separation (i.e., separation of security functions from non-security functions) in a number of ways, including, for example, through the provision of security kernels via processor rings or processor modes. For non-kernel code, security function isolation is often achieved through file system protections that serve to protect the code on disk, and address space protections that protect executing code. Information systems restrict access to security functions through the use of access control mechanisms and by implementing least privilege capabilities. While the ideal is for all of the code within the security function isolation boundary to only contain security-relevant code, it is sometimes necessary to include non-security functions within the isolation boundary as an exception.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** 1 TAC 202.22(1, 2); DIR Security Control Standards Catalog. **Federal**: FBI CJIS CSP v5.9.	AC-3, AC-6, AC-25, CM-2, CM-4, SA-4, SA-5, SA-8, SA-15, SA-17, SC-2, SC-7, SC-32, SC-39, SI-16.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing security function isolation; list of security functions to be isolated from non-security functions; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; system developer.

Test: Separation of security functions from non-security functions within the system.

SC-04: INFORMATION IN SHARED RESOURCES

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The information system prevents unauthorized and unintended information transfer via shared system resources.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Ensure that the information system does not share resources that are used to interface with systems operating at different security levels.

Std.02 — Ensure that system resources shared between two or more users are released back to the information system and are protected from accidental or purposeful disclosure.

SUPPLEMENTAL GUIDANCE

Preventing unauthorized and unintended information transfer via shared system resources stops information produced by the actions of prior users or roles (or the actions of processes acting on behalf of prior users or roles) from being available to current users or roles (or current processes acting on behalf of current users or roles) that obtain access to shared system resources after those resources have been released back to the system. Information in shared system resources also applies to encrypted representations of information. In other contexts, control of information in shared system resources is referred to as object reuse and residual information protection. Information in shared system resources does not address information remanence, which refers to the residual representation of data that has been nominally deleted; covert channels (including storage and timing channels), where shared system resources are manipulated to violate information flow restrictions; or components within systems for which there are only single users or roles.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FBI CJIS CSP v5.9.	AC-3, AC-4, SA-8.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing information protection in shared system resources; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; system developer.

Test: Automated mechanisms preventing unauthorized and unintended transfer of information via shared system resources.

SC-05: DENIAL OF SERVICE PROTECTION

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The information system:

a. Protect against or limit the effects of the following types of denial-of-service events: events as defined in Std.03; and

b. Employ the following controls to achieve the denial-of-service objective: controls as defined in Std.04.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — The DFPS Commissioner or his/her designated representative and Information Security Officer shall establish a security strategy that includes perimeter protection. [Source: DIR Control Standards Catalog SC-5]

Std.02 — The Department of Information Resources (DIR) will provide security information management services to include external network monitoring, scanning, and alerting for state organizations that utilize state information resources as specified in Chapters 2054 and 2059, Government Code. Perimeter security controls may include some or all of the following components: DMZ, firewall, intrusion detection or prevention system, or router. [Source: DIR Control Standards Catalog SC-5]

Std.03 — Protect against denial-of-service events against which preventive or limiting measures must be taken, including:

a. Consumption of scarce, limited, or non-renewable resources;

b. Destruction or alteration of configuration information; and

c. Physical destruction or alteration of network components. [Source: SP 800-82]

Std.04 — Employ applicable compensating controls, including:

a. The use of tools and configuration settings at boundaries to prevent denial of service events, including:
    1. IDS/IPS;
    2. Packet filtering; and
    3. Bandwidth limiting.

b. Monitoring

c. Operating in "safe mode" upon loss of communication;

d. Alternate communications services;

e. Securing and separating configuration backups; and

f. Alternate processing sites and services.

SUPPLEMENTAL GUIDANCE
Specific details about event types can be found at us-cert.gov, https://nvd.nist.gov/home, or other sources of threat intelligence per PM-16. Denial-of-service events may occur due to a variety of internal and external causes, such as an attack by an adversary or a lack of planning to support organizational needs with respect to capacity and bandwidth. Such attacks can occur across a wide range of network protocols (e.g., IPv4, IPv6). A variety of technologies are available to limit or eliminate the origination and effects of denial-of-service events. For example, boundary protection devices can filter certain types of packets to protect system components on internal networks from being directly affected by or the source of denial-of-service attacks. Employing increased network capacity and bandwidth combined with service redundancy also reduces the susceptibility to denial-of-service events.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: NIST SP 800-189; FBI CJIS CSP v5.9.	CP-2, IR-4, SC-6, SC-7, SC-40.

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: System and communications protection policy; procedures addressing denial-of-service protection; system design documentation; list of denial-of-service attacks requiring employment of security safeguards to protect against or limit effects of such attacks; list of security safeguards protecting against or limiting the effects of denial-of-service attacks; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records. Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with incident response responsibilities; system developer. Test: Automated mechanisms protecting against or limiting the effects of denial-of-service attacks.

SC-05(01): RESTRICT INTERNAL USERS

Priority: P1	
Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS
The information system restricts the ability of individuals to launch denial of service attacks against other information systems.
AGENCY IMPLEMENTATION STANDARDS
None.
SUPPLEMENTAL GUIDANCE

Restricting the ability of individuals to launch denial of service attacks requires that the mechanisms used for such attacks are unavailable. Individuals of concern can include, for example, hostile insiders or external adversaries that have successfully breached the information system and are using the system as a platform to launch cyber-attacks on third parties. Organizations can restrict the ability of individuals to connect and transmit arbitrary information on the transport medium (i.e., network, wireless spectrum). Organizations can also limit the ability of individuals to use excessive information system resources. Protection against individuals having the ability to launch denial of service attacks may be implemented on specific information systems or on boundary devices prohibiting egress to potential target systems.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FBI CJIS CSP v5.9.	None.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing denial-of-service protection; system design documentation; list of denial-of-service attacks launched by individuals against systems; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with incident response responsibilities; system developer.

Test: Automated mechanisms restricting the ability to launch denial-of-service attacks against other systems.

SC-05(02): CAPACITY, BANDWIDTH, AND REDUNDANCY

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding denial of service attacks.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Managing excess capacity ensures that sufficient capacity is available to counter flooding attacks. Managing excess capacity may include, for example, establishing selected usage priorities, quotas, or partitioning.

REFERENCES	RELATED CONTROLS

Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FBI CJIS CSP v5.9.	None.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing denial-of-service protection; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with incident response responsibilities; system developer.

Test: Automated mechanisms implementing management of system bandwidth, capacity, and redundancy to limit the effects of information flooding denial-of-service attacks.

SC-05(03): DETECTION AND MONITORING

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization:

a. Employs monitoring tools to detect indicators of denial of service attacks against the information system; and

b. Monitors information system resources to determine if sufficient resources exist to prevent effective denial of service attacks.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Organizations consider utilization and capacity of information system resources when managing risk from denial of service due to malicious attacks. Denial of service attacks can originate from external or internal sources. Information system resources sensitive to denial of service include, for example, physical disk storage, memory, and CPU cycles. Common safeguards to prevent denial of service attacks related to storage utilization and capacity include, for example, instituting disk quotas, configuring information systems to automatically alert administrators when specific storage capacity thresholds are reached, using file compression technologies to maximize available storage space, and imposing separate partitions for system and user data.

REFERENCES	**RELATED CONTROLS**

Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FBI CJIS CSP v5.9.	CA-7, SI-4.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing denial-of-service protection; system design documentation; system monitoring tools and techniques documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with detection and monitoring responsibilities.

Test: Automated mechanisms/tools implementing system monitoring for denial-of-service attacks.

SC-06: RESOURCE AVAILABILITY

Priority: P1

Baseline(s): N/A	Overlay(s): CJIS

CONTROL REQUIREMENTS

The information system protects the availability of resources by allocating resources by priority and/or quota.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Priority protection helps prevent lower-priority processes from delaying or interfering with the information system servicing any higher-priority processes. Quotas prevent users or processes from obtaining more than predetermined amounts of resources. This control does not apply to information system components for which there are only single users/roles.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FBI CJIS CSP v5.9.	SC-5.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing prioritization of system resources; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; system developer.

Test: Automated mechanisms supporting and/or implementing resource allocation capability; safeguards employed to protect availability of resources.

SC-07: BOUNDARY PROTECTION

Priority: P1

Baseline(s): N/A	Overlay(s): CJIS

CONTROL REQUIREMENTS

The information system:

a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;

b. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal organizational networks; and

c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — System Security Plans (SSPs) must include:

a. A complete, up-to-date network diagram and/or inventory of the system's boundaries;

b. Logging frequency to review logs and security events for all servers and system components providing security functions (for example, firewalls, intrusion-detection systems/intrusion prevention systems) to identify anomalies or suspicious activity; and

c. Methods to prevent the unauthorized release of information outside the information system boundary if an operational failure of the boundary protection mechanisms occurs.

Std.02 — Network communications must deny all by default and permit by exception for both inbound and outbound network communications traffic.

Std.03 — Separate subnetworks should be established as separate physical network interfaces for publicly-accessible system components

Std.04 — Limit inbound Internet traffic to IP addresses within the DMZ.

SUPPLEMENTAL GUIDANCE

Managed interfaces include gateways, routers, firewalls, guards, network-based malicious code analysis, virtualization systems, or encrypted tunnels implemented within a security architecture. Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs.

Restricting or prohibiting interfaces within organizational systems includes restricting external web traffic to designated web servers within managed interfaces, prohibiting external traffic that appears to be spoofing internal addresses, and prohibiting internal traffic that appears to be spoofing external addresses. SP 800-189 provides additional information on source address validation techniques to prevent ingress and egress of traffic with spoofed addresses. Commercial telecommunications services are provided by network components and consolidated management systems shared by customers. These services may also include third party- provided access lines and other service elements. Such services may represent sources of increased risk despite contract security provisions. Boundary protection may be implemented as a common control for all or part of an organizational network such that the boundary to be protected is greater than a system-specific boundary (i.e., an authorization boundary).

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; FIPS 199; NIST SP 800-37, 800-41, 800-77, 800-189; FBI CJIS CSP v5.9.	AC-4, AC-17, AC-18, AC-19, AC-20, AU-13, CA-3, CM-2, CM-4, CM-7, CM-10, CP-8, CP-10, IR-4, MA-4, PE-3, PL-8, PM-12, SA-8, SA-17, SC-5, SC-26, SC-32, SC-35, SC-43.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the system; system design documentation; boundary protection hardware and software; system configuration settings and associated documentation; enterprise security architecture documentation; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with boundary protection responsibilities.

Test: Automated mechanisms implementing boundary protection capabilities.

SC-07(03): ACCESS POINTS

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization limits the number of external network connections to the information system.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Document, verify and control connections to and use of external systems. [Source: SP 800-171 3.1.21/ CSF ID.AM-4]

SUPPLEMENTAL GUIDANCE

Limiting the number of external network connections facilitates more comprehensive monitoring of inbound and outbound communications traffic. The Trusted Internet Connection (TIC) initiative is an example of limiting the number of external network connections. The Trusted Internet Connection initiative is an example of a federal

guideline that requires limits on the number of external network connections. Limiting the number of external network connections to the system is important during transition periods from older to newer technologies (e.g., transitioning from IPv4 to IPv6 network protocols). Such transitions may require implementing the older and newer technologies simultaneously during the transition period and thus increase the number of access points to the system.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; FIPS 199; NIST SP 800-37, 800-41, 800-77, 800-189; FBI CJIS CSP v5.9.	AC-4, AC-17, AC-18, AC-19, AC-20, AU-13, CA-3, CM-2, CM-4, CM-7, CM-10, CP-8, CP-10, IR-4, MA-4, PE-3, PL-8, PM-12, SA-8, SA-17, SC-5, SC-26, SC-32, SC-35, SC-43.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing boundary protection; system design documentation; boundary protection hardware and software; system architecture and configuration documentation; system configuration settings and associated documentation; communications and network traffic monitoring logs; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with boundary protection responsibilities.

Test: Automated mechanisms implementing boundary protection capabilities; automated mechanisms limiting the number of external network connections to the system.

SC-07(04): EXTERNAL TELECOMMUNICATIONS SERVICES

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization:

a. Implement a managed interface for each external telecommunication service;

b. Establish a traffic flow policy for each managed interface;

c. Protect the confidentiality and integrity of the information being transmitted across each interface;

d. Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need;

e. Review exceptions to the traffic flow policy at least once every 180 days and upon implementation of a major new system and remove exceptions that are no longer supported by an explicit mission or business need;

f. Prevent unauthorized exchange of control plane traffic with external networks;

g. Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks; and

h. Filter unauthorized control plane traffic from external networks.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

External telecommunications services can provide data and/or voice communications services. Examples of control plane traffic include Border Gateway Protocol (BGP) routing, Domain Name System (DNS), and management protocols. See SP 800-189 for additional information on the use of the resource public key infrastructure (RPKI) to protect BGP routes and detect unauthorized BGP announcements.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; FIPS 199; NIST SP 800-37, 800-41, 800-77, 800-189; FBI CJIS CSP v5.9.	AC-3, SC-8, SC-20, SC-21, SC-22.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; traffic flow policy; information flow control policy; procedures addressing boundary protection; system security architecture; system design documentation; boundary protection hardware and software; system architecture and configuration documentation; system configuration settings and associated documentation; records of traffic flow policy exceptions; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with boundary protection responsibilities.

Test: Organizational processes for documenting and reviewing exceptions to the traffic flow policy; organizational processes for removing exceptions to the traffic flow policy; automated mechanisms implementing boundary protection capabilities; managed interfaces implementing traffic flow policy.

SC-07(05): DENY BY DEFAULT — ALLOW BY EXCEPTION

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization denies network communications traffic by default and allow network communications traffic by exception at managed interfaces.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Establish and implement firewall and router configuration standards that include requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone.

SUPPLEMENTAL GUIDANCE

Denying by default and allowing by exception applies to inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those system connections that are essential and approved are allowed. Deny by default, allow by exception also applies to a system that is connected to an external system.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; FIPS 199; NIST SP 800-37, 800-41, 800-77, 800-189; FBI CJIS CSP v5.9.	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing boundary protection; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with boundary protection responsibilities.

Test: Automated mechanisms implementing traffic management at managed interfaces.

SC-07(07): SPLIT TUNNELING FOR REMOTE DEVICES

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization prevents split tunneling for remote devices connecting to organizational systems unless the split tunnel is securely provisioned using the following organization-defined safeguards: split tunneling is not authorized unless explicitly approved by the DFPS Chief Information Security Officer or their delegate.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

This control enhancement is implemented within remote devices (e.g., notebook computers) through configuration settings to disable split tunneling in those devices, and by preventing those configuration settings from being readily configurable by users. This control enhancement is implemented within the information

system by the detection of split tunneling (or of configuration settings that allow split tunneling) in the remote device, and by prohibiting the connection if the remote device is using split tunneling. Split tunneling might be desirable by remote users to communicate with local information system resources such as printers/file servers. However, split tunneling would in effect allow unauthorized external connections, making the system more vulnerable to attack and to exfiltration of organizational information. The use of VPNs for remote connections, when adequately provisioned with appropriate security controls, may provide the organization with sufficient assurance that it can effectively treat such connections as non-remote connections from the confidentiality and integrity perspective. VPNs thus provide a means for allowing non-remote communications paths from remote devices. The use of an adequately provisioned VPN does not eliminate the need for preventing split tunneling.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; FIPS 199; NIST SP 800-37, 800-41, 800-77, 800-189; FBI CJIS CSP v5.9.	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing boundary protection; system design documentation; system hardware and software; system architecture; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with boundary protection responsibilities.

Test: Automated mechanisms implementing boundary protection capabilities; automated mechanisms supporting/restricting non-remote connections.

SC-07(08): ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization route all internal communications traffic to any external networks through authenticated proxy servers at managed interfaces.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

External networks are networks outside of organizational control. A proxy server is a server (i.e., information system or application) that acts as an intermediary for clients requesting information system resources (e.g., files, connections, web pages, or services) from other organizational servers. Client requests established through

an initial connection to the proxy server are evaluated to manage complexity and to provide additional protection by limiting direct connectivity. Web content filtering devices are one of the most common proxy servers providing access to the Internet. Proxy servers support logging individual Transmission Control Protocol (TCP) sessions and blocking specific Uniform Resource Locators (URLs), domain names, and Internet Protocol (IP) addresses. Web proxies can be configured with organization-defined lists of authorized and unauthorized websites.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; FIPS 199; NIST SP 800-37, 800-41, 800-77, 800-189; FBI CJIS CSP v5.9.	AC-3.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing boundary protection; system design documentation; system hardware and software; system architecture; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records

Interview: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with boundary protection responsibilities.

Test: Automated mechanisms implementing traffic management through authenticated proxy servers at managed interfaces.

SC-07(11): RESTRICT INCOMING COMMUNICATIONS TRAFFIC

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The information system only allows incoming communications from authorized sources to be routed to authorized destinations.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

This control enhancement provides determinations that source and destination address pairs represent authorized/allowed communications. Such determinations can be based on several factors including, for example, the presence of source/destination address pairs in lists of authorized/allowed communications, the absence of address pairs in lists of unauthorized/disallowed pairs, or meeting more general rules for authorized/allowed source/destination pairs.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; FIPS 199; NIST SP 800-37, 800-41, 800-77, 800-189; FBI CJIS CSP v5.9.	AC-3.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing boundary protection; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with boundary protection responsibilities.

Test: Automated mechanisms implementing boundary protection capabilities with respect to source/destination address pairs.

SC-07(12): HOST-BASED PROTECTION

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization implements defined, host-based boundary protection mechanisms at defined information system components, including servers, workstations, and mobile devices.

For cloud-based applications, the organization implements FedRAMP (or TX-Ramp) defined host-based boundary protection mechanisms at FedRAMP defined information system components.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Host-based boundary protection mechanisms include, for example, host-based firewalls. Information system components employing host-based boundary protection mechanisms include, for example, servers, workstations, and mobile devices.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog.	N/A

Federal: FedRAMP Baselines; OMB A-130; FIPS 199; NIST SP 800-37, 800-41, 800-77, 800-189; FBI CJIS CSP v5.9.	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing boundary protection; system design documentation; boundary protection hardware and software; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with boundary protection responsibilities; system users.

Test: Automated mechanisms implementing host-based boundary protection capabilities.

SC-07(13) ISOLATION OF SECURITY TOOLS, MECHANISMS, AND SUPPORT COMPONENTS

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization defines key information security tools, mechanisms, and support components associated with system and security administration; and isolates those tools, mechanisms, and support components from other internal information system components via physically or logically separate subnets.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Physically separate subnetworks with managed interfaces are useful, for example, in isolating computer network defenses from critical operational processing networks to prevent adversaries from discovering the analysis and forensics techniques of organizations.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; FIPS 199; NIST SP 800-37, 800-41, 800-77, 800-189; FBI CJIS CSP v5.9.	SC-2, SC-3.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing boundary protection; system design documentation; system hardware and software; system architecture; system configuration settings and associated documentation; list of security tools and support components to be isolated from other internal system components; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with boundary protection responsibilities.

Test: Automated mechanisms supporting and/or implementing isolation of information security tools, mechanisms, and support components.

SC-07(14): PROTECT AGAINST UNAUTHORIZED PHYSICAL CONNECTIONS

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization protects against unauthorized physical connections at those organization-defined managed interfaces necessary to prevent unauthorized physical access, tampering, and theft of CJI and other sensitive information.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Information systems operating at different security categories or classification levels may share common physical and environmental controls, since the systems may share space within organizational facilities. In practice, it is possible that these separate information systems may share common equipment rooms, wiring closets, and cable distribution paths. Protection against unauthorized physical connections can be achieved, for example, by employing clearly identified and physically separated cable trays, connection frames, and patch panels for each side of managed interfaces with physical access controls enforcing limited authorized access to these items.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; FIPS 199; NIST SP 800-37, 800-41, 800-77, 800-189; FBI CJIS CSP v5.9.	PE-4, PE-19.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing boundary protection; system design documentation; system hardware and software; system architecture; system configuration settings and associated documentation; facility communications and wiring diagram system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with boundary protection responsibilities.

Test: Automated mechanisms supporting and/or implementing protection against unauthorized physical connections.

SC-07(18): FAIL SECURE

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The information system prevents systems from entering unsecure states in the event of an operational failure of a boundary protection device.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Fail secure is a condition achieved by employing mechanisms to ensure that in the event of operational failures of boundary protection devices at managed interfaces, systems do not enter into unsecure states where intended security properties no longer hold. Managed interfaces include routers, firewalls, and application gateways that reside on protected subnetworks (commonly referred to as demilitarized zones). Failures of boundary protection devices cannot lead to or cause information external to the devices to enter the devices nor can failures permit unauthorized information releases.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; FIPS 199; NIST SP 800-37, 800-41, 800-77, 800-189; FBI CJIS CSP v5.9.	CP-2, CP-12, SC-24.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing boundary protection; system design documentation; system architecture; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with boundary protection responsibilities.

Test: Automated mechanisms supporting and/or implementing secure failure.

SC-07(19): BLOCK COMMUNICATION FROM NON-ORGANIZATIONALLY CONFIGURED HOSTS

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The information system blocks both inbound and outbound communications traffic between communication clients that are independently configured by end users and external service providers.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Communication clients independently configured by end users and external service providers include, for example, instant messaging clients. Traffic blocking does not apply to communication clients that are configured by organizations to perform authorized functions.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; FIPS 199; NIST SP 800-37, 800-41, 800-77, 800-189; FBI CJIS CSP v5.9.	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing boundary protection; system design documentation; system hardware and software; system architecture; system configuration settings and associated documentation; list of communication clients independently configured by end users and external service providers; system audit records; system security plan; other relevant documents or records

Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with boundary protection responsibilities.

Test: Automated mechanisms supporting and/or implementing the blocking of inbound and outbound communications traffic between communication clients independently configured by end users and external service provider.

SC-07(24): PERSONALLY IDENTIFIABLE INFORMATION

Priority: P1

Baseline(s): Moderate, High	Overlay(s): Privacy

CONTROL REQUIREMENTS

For systems that process personally identifiable information:

a. Apply the following processing rules to data elements of personally identifiable information: processing rules in accordance with PT-02;
b. Monitor for permitted processing at the external interfaces to the system and at key internal boundaries within the system;
c. Document each processing exception; and
d. Review and remove exceptions that are no longer supported.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Document processing rules in the System Security Plan (SSP).

SUPPLEMENTAL GUIDANCE

Managing the processing of personally identifiable information is an important aspect of protecting an individual's privacy. Applying, monitoring for, and documenting exceptions to processing rules ensure that personally identifiable information is processed only in accordance with established privacy requirements.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** Bus. & Comm. Code 521; DIR Security Control Standards Catalog. **Federal**: OMB A-130; FIPS 199; NIST SP 800-37, 800-41, 800-77, 800-189; FBI CJIS CSP v5.9.	PT-2, SI-15.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing boundary protection; personally identifiable information processing policies; list of key internal boundaries of the system; system design documentation; system configuration settings and associated documentation; enterprise security and privacy architecture documentation; system audit records; system security plan; privacy plan; personally identifiable information inventory documentation; data mapping documentation; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security and privacy responsibilities; system developer; organizational personnel with boundary protection responsibilities.

Test: Automated mechanisms implementing boundary protection capabilities.

SC-08: TRANSMISSION CONFIDENTIALITY AND INTEGRITY

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS, Privacy

CONTROL REQUIREMENTS

The information system protects the confidentiality and integrity of transmitted information.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Confidential information that is transmitted over a public network (e.g., the Internet) must be encrypted. DFPS may also choose to implement encryption for other data classifications. [Source: DIR Control Standards Catalog SC-8]

Std.02 — Sensitive information that is transmitted over a public network (e.g., the Internet) must be encrypted.

Std.03 — Implement cryptographic mechanisms compliant with SC-13 to prevent unauthorized disclosure of information and detect changes to information during transmission.

SUPPLEMENTAL GUIDANCE

Protecting the confidentiality and integrity of transmitted information applies to internal and external networks as well as any system components that can transmit information, including servers, notebook computers, desktop computers, mobile devices, printers, copiers, scanners, facsimile machines, and radios. Unprotected communication paths are exposed to the possibility of interception and modification. Protecting the confidentiality and integrity of information can be accomplished by physical or logical means. Physical protection can be achieved by using protected distribution systems. A protected distribution system is a wireline or fiber-optics telecommunications system that includes terminals and adequate electromagnetic, acoustical, electrical, and physical controls to permit its use for the unencrypted transmission of classified information. Logical protection can be achieved by employing encryption techniques.

Organizations that rely on commercial providers who offer transmission services as commodity services rather than as fully dedicated services may find it difficult to obtain the necessary assurances regarding the implementation of needed controls for transmission confidentiality and integrity. In such situations, organizations determine what types of confidentiality or integrity services are available in standard, commercial telecommunications service packages. If it is not feasible to obtain the necessary controls and assurances of control effectiveness through appropriate contracting vehicles, organizations can implement appropriate compensating controls.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FIPS 140, 197; NIST SP 800-52, 800-77, 800-81-2, 800-113, 800-177; NIST IR 8023; FBI CJIS CSP v5.9.	AC-17, AC-18, AU-10, IA-3, IA-8, IA-9, MA-4, PE-4, SA-4, SA-8, SC-7, SC-16, SC-20, SC-23, SC-28.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing transmission confidentiality and integrity; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records

Interview: System/network administrators; organizational personnel with information security responsibilities; system developer.

Test: Automated mechanisms supporting and/or implementing transmission confidentiality and/or integrity.

SC-08(01): CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The information system implements cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Any transmitted data containing Sensitive, Confidential, or Regulated information must be encrypted in accordance with SC-13.

SUPPLEMENTAL GUIDANCE

Encryption protects information from unauthorized disclosure and modification during transmission. Cryptographic mechanisms that protect the confidentiality and integrity of information during transmission include TLS and IPSec. Cryptographic mechanisms used to protect information integrity include cryptographic hash functions that have applications in digital signatures, checksums, and message authentication codes.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FIPS 140, 197; NIST SP 800-52, 800-77, 800-81-2, 800-113, 800-177; NIST IR 8023; FBI CJIS CSP v5.9.	SC-12, SC-13.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing transmission confidentiality and integrity; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; system developer.

Test: Cryptographic mechanisms supporting and/or implementing transmission confidentiality and/or integrity; automated mechanisms supporting and/or implementing alternative physical safeguards; organizational processes for defining and implementing alternative physical safeguards.

SC-08(02): PRE / POST TRANSMISSION HANDLING

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The information system maintains the confidentiality and integrity of information during preparation for transmission and during reception.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — The information system in preparation for transmission and during reception maintains the confidentiality and integrity of information during:

- aggregation;

- packaging;

- transformation.

SUPPLEMENTAL GUIDANCE

Information can be either unintentionally or maliciously disclosed or modified during preparation for transmission or during reception including, for example, during aggregation, at protocol transformation points, and during packing/unpacking. These unauthorized disclosures or modifications compromise the confidentiality or integrity of the information.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FIPS 140, 197; NIST SP 800-52, 800-77, 800-81-2, 800-113, 800-177; NIST IR 8023; FBI CJIS CSP v5.9.	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing transmission confidentiality and integrity; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; system developer.

Test: Automated mechanisms supporting and/or implementing transmission confidentiality and/or integrity.

SC-09: TRANSMISSION CONFIDENTIALITY

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

This control is withdrawn and incorporated into SC-08 but still referenced in the FBI CJIS Security Policy v5.9. Please see SC-08.

SC-10: NETWORK DISCONNECT

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The information system terminates the network connection associated with a communications session at the end of the session or after the period defined in Std.01 of inactivity.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Configure network connections to disconnect according to the following guide:

a. For low baseline: 60 minutes of inactivity;

b. For moderate baseline: 30 minutes of inactivity;

c. For high baseline: 10 minutes of inactivity.

Require re-authentication before allowing access to the system after the network connection has been terminated due to inactivity.

SUPPLEMENTAL GUIDANCE

Network disconnect applies to internal and external networks. Terminating network connections associated with specific communications sessions includes de-allocating TCP/IP address or port pairs at the operating system level and de-allocating the networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. Periods of inactivity may be established by organizations and include time periods by type of network access or for specific network accesses.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FBI CJIS CSP v5.9.	AC-17, SC-23.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing network disconnect; system design documentation; security plan; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; system developer.

Test: Automated mechanisms supporting and/or implementing network disconnect capability.

SC-11: TRUSTED PATH

Priority: P1

Baseline(s): N/A	Overlay(s): CJIS

CONTROL REQUIREMENTS

The information system:

a. Provide a physically and/or logically isolated trusted communications path for communications between the user and the trusted components of the system; and

b. Permit users to invoke the trusted communications path for communications between the user and the following security functions of the system, including at a minimum, authentication and re-authentications defined in the system security plan (SSP).

For cloud-based applications, the information system establishes a trusted communications path between the user and the FedRAMP security functions of the system, to include at a minimum, information system authentication and re-authentication.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Trusted paths are mechanisms by which users (through input devices) can communicate directly with security functions of information systems with the requisite assurance to support information security policies. The mechanisms can be activated only by users or the security functions of organizational information systems. User responses via trusted paths are protected from modifications by or disclosure to untrusted applications. Organizations employ trusted paths for high-assurance connections between security functions of information systems and users (e.g., during system logons). Enforcement of trusted communications paths is typically provided via an implementation that meets the reference monitor concept.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog.	AC-16, AC-25, SC-12, SC-23.

Federal: FBI CJIS CSP v5.9.	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing trusted communication paths; security plan; system design documentation; system configuration settings and associated documentation; assessment results from independent, testing organizations; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; system developer.

Test: Automated mechanisms supporting and/or implementing trusted communication paths.

SC-12: CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with the key management requirements SC-13 and applicable System Security Plans (SSPs).

AGENCY IMPLEMENTATION STANDARDS

Std.01 — When cryptography is required and employed within the information system, DFPS must establish and manage cryptographic keys using automated mechanisms with supporting procedures or manual procedures. [Source: DIR Control Standards Catalog SC- 12]

Std.02 — For websites and mobile applications, only procure, or otherwise implement, certificates from PKI Service Providers that appear on the DIR "Approved List of PKI Service Providers." [Source: 1 TAC 203.25(b)]

Std.03 — Protect all cryptographic keys against modification, loss, and destruction; protect secret and private keys against unauthorized disclosure. Limit cryptographic keys to the fewest number of custodians necessary. Physically protect equipment used to generate, store, and archive keys, and store encryption keys separately from encrypted data. [Source: Hitrust 10.g Key Management]

Std.04 — For Web and mobile apps, the name on the certificate should match the fully qualified domain name (FQDN) of the website.

SUPPLEMENTAL GUIDANCE

Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. Organizations define key management requirements in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and specify appropriate options, parameters, and levels. Organizations manage trust stores to ensure that only approved trust anchors are part of such trust stores. This includes certificates with visibility external to organizational systems and certificates related to the internal operations of systems. NIST CMVP and NIST CAVP

provide additional information on validated cryptographic modules and algorithms that can be used in cryptographic key management and establishment.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** 1 TAC 203.25(b); DIR Security Control Standards Catalog. **Federal**: FIPS 140; NIST SP 800-56A, 800-56B, 800-56C, 800-57-1, 800-57-2, 800-57-3, 800-63-3; NIST IR 7956, 7966; FBI CJIS CSP v5.9.	AC-17, AU-9, AU-10, CM-3, IA-3, IA-7, SA-4, SA-8, SA-9, SC-8, SC-11, SC-12, SC-13, SC-17, SC-20, SC-37, SC-40, SI-3, SI-7.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing cryptographic key establishment and management; system design documentation; cryptographic mechanisms; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with responsibilities for cryptographic key establishment and/or management.

Test: Automated mechanisms supporting and/or implementing cryptographic key establishment and management.

SC-12(01): AVAILABILITY

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization maintains availability of information in the event of the loss of cryptographic keys by users.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Mechanisms must be employed to:

a. Prohibit the use of encryption keys that are not recoverable by authorized personnel;

b. Require approval by senior management (as defined in applicable System Security Plans (SSPs)) to authorize recovery of keys by other than the key owner; and

c. Comply with approved cryptography standards (see SC-13).

SUPPLEMENTAL GUIDANCE

Escrowing of encryption keys is a common practice for ensuring availability in the event of key loss. A forgotten passphrase is an example of losing a cryptographic key.

REFERENCES	RELATED CONTROLS

Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FIPS 140; NIST SP 800-56A, 800-56B, 800-56C, 800-57-1, 800-57-2, 800-57-3, 800-63-3; NIST IR 7956, 7966; FBI CJIS CSP v5.9.	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing cryptographic key establishment, management, and recovery; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with responsibilities for cryptographic key establishment or management.

Test: Automated mechanisms supporting and/or implementing cryptographic key establishment and management.

SC-12(02): SYMMETRIC KEYS

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization produces, controls, and distributes symmetric cryptographic keys using NIST FIPS-compliant key management technology and processes.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS systems must implement encryption algorithms that are FIPS 140-2 certified and use a symmetric cipher key strength of at least 128 bit strength.

NOTE: Subsequent versions of approved cryptographic modules that are under current review for FIPS 140-2 compliancy can be used in the interim until certification is complete.

SUPPLEMENTAL GUIDANCE

Escrowing of encryption keys is a common practice for ensuring availability in the event of key loss. A forgotten passphrase is an example of losing a cryptographic key.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog.	N/A

Federal: FIPS 140; NIST SP 800-56A, 800-56B, 800-56C, 800-57-1, 800-57-2, 800-57-3, 800-63-3; NIST IR 7956, 7966; FBI CJIS CSP v5.9.	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing cryptographic key establishment and management; system design documentation; system configuration settings and associated documentation; system audit records; list of FIPS-validated cryptographic products; list of NSA-approved cryptographic products; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with responsibilities for cryptographic key establishment or management.

Test: Automated mechanisms supporting and/or implementing symmetric cryptographic key establishment and management.

SC-12(03): ASYMMETRIC KEYS

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization produces, controls, and distributes asymmetric cryptographic keys using NIST-approved key management technology and processes; approved PKI Class 3 certificates or prepositioned keying material; approved PKI Class 3 or Class 4 certificates and hardware security tokens protecting the user's private key.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS systems must implement encryption algorithms that are FIPS 140-2 certified and use a symmetric cipher key strength of at least 128 bit strength.

NOTE: Subsequent versions of approved cryptographic modules that are under current review for FIPS 140-2 compliancy can be used in the interim until certification is complete.

SUPPLEMENTAL GUIDANCE

NIST SP 800-56A, SP 800-56B, and SP 800-56C provide guidance on cryptographic key establishment schemes and key derivation methods. NIST SP 800-57-1, SP 800-57-2, and SP 800-57-3 provide guidance on cryptographic key management

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog.	N/A

Federal: FIPS 140; NIST SP 800-56A, 800-56B, 800-56C, 800-57-1, 800-57-2, 800-57-3, 800-63-3; NIST IR 7956, 7966; FBI CJIS CSP v5.9.	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing cryptographic key establishment and management; system design documentation; system configuration settings and associated documentation; system audit records; list of NSA-approved cryptographic products; list of approved PKI Class 3 and Class 4 certificates; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with responsibilities for cryptographic key establishment or management; organizational personnel with responsibilities for PKI certificates.

Test: Automated mechanisms supporting and/or implementing asymmetric cryptographic key establishment and management.

SC-13: CRYPTOGRAPHIC PROTECTION

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Determine the cryptographic uses in accordance with Stds.01-04; and

b. Implement the following types of cryptography required for each specified cryptographic use: DFPS systems with Sensitive, Confidential or Controlled data must implement encryption in accordance with Std.05.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Encryption requirements for information storage devices and data transmissions, as well as specific requirements for portable devices, removable media, and encryption key standards and management, shall be based on documented DFPS risk management decisions. [Source: DIR Control Standards Catalog SC-13]

Std.02 — Sensitive, Confidential or Conrolled information that is transmitted over a public network (e.g., the Internet) must be encrypted. [Source: DIR Control Standards Catalog SC- 13]

Std.03 — Sensitive, Confidential or Controlled information stored in a public location that is directly accessible without compensating controls in place (e.g., FTP without access control) must be encrypted. [Source: DIR Control Standards Catalog SC-13]

Std.04 — Confidential or regulated information must be encrypted if copied to, or stored on, a portable computing device, removable media, or a non-DFPS owned computing device. [Source: DIR Control Standards Catalog SC-13]

Std.05 — DFPS systems must implement encryption algorithms to the level recommend by the FBI CJIS Security Policy section in Section 5.10.1.2.1 use a symmetric cipher that is FIPS 197 certified (AES) and at least 256 bit

strength. Recommendations for FIPS 197 certified can be found on the Commercial National Security Algorithm (CNSA) Suite: https://apps.nsa.gov/iaarchive/programs/iad-initiatives/cnsa-suite.cfm

Std.06 — DFPS may also choose to implement additional protections, which may include encryption, for other data classifications. [Source: DIR Control Standards Catalog SC-13]

SUPPLEMENTAL GUIDANCE

NIST SP 800-56A, SP 800-56B, and SP 800-56C provide guidance on cryptographic key establishment schemes and key derivation methods. NIST SP 800-57-1, SP 800-57-2, and SP 800-57-3 provide guidance on cryptographic key management

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FIPS 140; FIPS 197; FBI CJIS CSP v5.9.	AC-2, AC-3, AC-7, AC-17, AC-18, AC-19, AU-9, AU-10, CM-11, CP-9, IA-3, IA-5, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SA-8, SA-9, SC-8, SC-12, SC-20, SC-23, SC-28, SC-40, SI-3, SI-7.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing cryptographic key establishment and management; system design documentation; system configuration settings and associated documentation; system audit records; list of NSA-approved cryptographic products; list of approved PKI Class 3 and Class 4 certificates; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with responsibilities for cryptographic key establishment or management; organizational personnel with responsibilities for PKI certificates.

Test: Automated mechanisms supporting and/or implementing asymmetric cryptographic key establishment and management.

SC-15: COLLABORATIVE COMPUTING DEVICES AND APPLICATIONS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Prohibit remote activation of collaborative computing devices and applications with the following exceptions: centrally managed dedicated devices located in DFPS-managed facilities for which remote activation is approved and documented in System Security Plans (SSPs); and

b. Provide an explicit indication of use to users physically present at the devices.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Collaborative computing devices must be disconnected by default and provide at least one explicit indicator of use when powered on and connected.

SUPPLEMENTAL GUIDANCE

Collaborative computing devices and applications include remote meeting devices and applications, networked white boards, cameras, and microphones. The explicit indication of use includes signals to users when collaborative computing devices and applications are activated.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FBI CJIS CSP v5.9.	AC-21, SC-42.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing collaborative computing; access control policy and procedures; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with responsibilities for managing collaborative computing devices.

Test: Automated mechanisms supporting and/or implementing the management of remote activation of collaborative computing devices; automated mechanisms providing an indication of use of collaborative computing device.

SC-15(01): PHYSICAL DISCONNECT

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

If collaborative computing is authorized, the information system provides physical disconnect of collaborative computing devices in a manner that supports ease of use.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Collaborative computing devices must be able to be physically disconnected quickly and with minimal effort.

SUPPLEMENTAL GUIDANCE

Failing to physically disconnect from collaborative computing devices can result in subsequent compromises of organizational information. Providing easy methods to physically disconnect from such devices after a

collaborative computing session helps to ensure that participants actually carry out the disconnect activity without having to go through complex and tedious procedures.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FBI CJIS CSP v5.9.	None.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing collaborative computing; access control policy and procedures; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with responsibilities for managing collaborative computing devices.

Test: Automated mechanisms supporting and/or implementing the physical disconnect of collaborative computing devices.

SC-16: TRANSMISSION OF SECURITY ATTRIBUTES

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

For systems processing CJIS data, the following additional Implementation Standard applies:

The information system associates FBI authorized originating agency identifier (ORI) with information exchanged between information systems and between system components.

AGENCY IMPLEMENTATION STANDARDS

Std.01 —An FBI authorized originating agency identifier (ORI) shall be used in each transaction on CJIS systems in order to identify the sending agency and to ensure the proper level of access for each transaction. The original identifier between the requesting agency and the CSA/SIB/Channeler shall be the ORI, and other agency identifiers, such as user identification or personal identifier, an access device mnemonic, or the Internet Protocol (IP) address. [Source: FBI CJIS CSP v5.9]

Std.02 — Agencies may act as a servicing agency and perform transactions on behalf of authorized agencies requesting the service. Servicing agencies performing inquiry transactions on behalf of another agency may do so using the requesting agency's ORI. Servicing agencies may also use their own ORI to perform inquiry transactions on behalf of a requesting agency if the means and procedures are in place to provide an audit trail for the current specified retention period. Because the agency performing the transaction may not necessarily be the same as the agency requesting the transaction, the CSA/SIB/Channeler shall ensure that the ORI for each transaction can be traced, via audit trail, to the specific agency which is requesting the transaction. [Source: FBI CJIS CSP v5.9]

Std.03 — Audit trails can be used to identify the requesting agency if there is a reason to inquire into the details surrounding why an agency ran an inquiry on a subject. Agencies assigned a P (limited access) ORI shall not use the full access ORI of another agency to conduct an inquiry transaction. [Source: FBI CJIS CSP v5.9]

SUPPLEMENTAL GUIDANCE

Security and privacy attributes can be explicitly or implicitly associated with the information contained in organizational systems or system components. Attributes are abstractions that represent the basic properties or characteristics of an entity with respect to protecting information or the management of personally identifiable information. Attributes are typically associated with internal data structures, including records, buffers, and files within the system. Security and privacy attributes are used to implement access control and information flow control policies; reflect special dissemination, management, or distribution instructions, including permitted uses of personally identifiable information; or support other aspects of the information security and privacy policies. Privacy attributes may be used independently or in conjunction with security attributes.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FBI CJIS CSP v5.9.	AC-3, AC-4, AC-16.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing the transmission of security and privacy attributes; access control policy and procedures; information flow control policy; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; privacy plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security and privacy responsibilities.

Test: Automated mechanisms supporting and/or implementing the transmission of security and privacy attributes between systems.

SC-16(01): INTEGRITY VALIDATION

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

For systems processing CJIS data, the following additional Implementation Standard applies:

The information system verifies the integrity of transmitted security and privacy attributes.

AGENCY IMPLEMENTATION STANDARDS

Std.01 – Any transmitted data containing Sensitive, Confidential, or Regulated information must be encrypted in accordance with SC-08

Std.02 – Any transmitted data containing Sensitive, Confidential, or Regulated information must provide irrefutable evidence that an individual (or process acting on behalf of an individual) has performed in accordance with AU-10.

SUPPLEMENTAL GUIDANCE

Part of verifying the integrity of transmitted information is ensuring that security and privacy attributes that are associated with such information have not been modified in an unauthorized manner. Unauthorized modification of security or privacy attributes can result in a loss of integrity for transmitted information.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FBI CJIS CSP v5.9.	AU-10, SC-8.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing the transmission of security and privacy attributes; access control policy and procedures; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; privacy plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security and privacy responsibilities.

Test: Automated mechanisms supporting and/or implementing verification of the integrity of transmitted security and privacy attributes.

SC-17: PUBLIC KEY INFRASTRUCTURE CERTIFICATES

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Issue public key certificates under a DFPS-approved certificate policy or obtain public key certificates from an approved service provider; and

b. Include only approved trust anchors in trust stores or certificate stores managed by the organization.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — State agencies shall only procure, or otherwise implement, certificates from PKI Service Providers that appear on the Texas Department of Information Resources "Approved List of PKI Service Providers." [Source: 1 TAC 202.35(b)]

Std.02 — Public key certificates must be issued using a secure process that both verifies the identity of the certificate holder and ensures that the certificate is issued to the intended party at the assurance level specified in DFPS Identification and Authentication Standard.

Std.03 — Certificates for internal system operations (for example, application-specific time services, desktops, internal servers) must use Active Directory certificates or others approved by DFPS and documented in the System Security Plan (SSP).

Std.04 — DFPS must provide oversight in the creation of Public Key Infrastructure (PKI) framework and services that provide the generation, production, distribution, control, revocation, recovery, and tracking of PKI certificates and their corresponding private keys.

Std.05 — PKI certificates must be encrypted using an approved algorithm as defined in SC-13. (See SC-13, Std.05).

Std.06 — PKI certificates must be valid for a maximum of 397 days.

SUPPLEMENTAL GUIDANCE

Public key infrastructure (PKI) certificates are certificates with visibility external to organizational systems and certificates related to the internal operations of systems, such as application-specific time services. In cryptographic systems with a hierarchical structure, a trust anchor is an authoritative source (i.e., a certificate authority) for which trust is assumed and not derived. A root certificate for a PKI system is an example of a trust anchor. A trust store or certificate store maintains a list of trusted root certificates.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; Identification and Authentication Standard. **State:** DIR Security Control Standards Catalog. **Federal**: NIST SP 800-32, 800-57-1, 800-57-2, 800-57-3, 800-63-3; FBI CJIS CSP v5.9.	AU-10, IA-5, SC-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing public key infrastructure certificates; public key certificate policy or policies; public key issuing process; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with responsibilities for issuing public key certificates; service providers.

Test: Automated mechanisms supporting and/or implementing the management of public key infrastructure certificates.

SC-18: MOBILE CODE

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Define acceptable and unacceptable mobile code and mobile code technologies; and

b. Authorize, monitor, and control the use of mobile code within the system.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - DFPS must document and define the mobile code technologies used in System Security Plans (SSPs).

Std.02 – The DFPS Chief Information Security Officer or their delegate reviews and approves System Security Plans (SSPs) on an annual basis.

SUPPLEMENTAL GUIDANCE

Mobile code includes any program, application, or content that can be transmitted across a network (e.g., embedded in an email, document, or website) and executed on a remote system. Decisions regarding the use of mobile code within organizational systems are based on the potential for the code to cause damage to the systems if used maliciously. Mobile code technologies include Java applets, JavaScript, HTML5, WebGL, and VBScript. Usage restrictions and implementation guidelines apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices, including notebook computers and smart phones. Mobile code policy and procedures address specific actions taken to prevent the development, acquisition, and introduction of unacceptable mobile code within organizational systems, including requiring mobile code to be digitally signed by a trusted source.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: NIST SP 800-28; FBI CJIS CSP v5.9.	AU-2, AU-12, CM-2, CM-6, SI-3.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing mobile code; mobile code implementation policy and procedures; list of acceptable mobile code and mobile code technologies; list of unacceptable mobile code and mobile technologies; authorization records; system monitoring records; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with responsibilities for managing mobile code.

Test: Organizational process for authorizing, monitoring, and controlling mobile code; automated mechanisms supporting and/or implementing the management of mobile code; automated mechanisms supporting and/or implementing the monitoring of mobile code.

SC-18(01): IDENTIFY UNACCEPTABLE CODE / TAKE CORRECTIVE ACTIONS

Priority: P1	
Baseline(s): Low, Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The information system identifies unacceptable mobile code in mobile devices that have a full-feature operating system (i.e. laptops or tables) and ensures, at a minimum the personal firewall performs the actions outlined in Std.01.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - A personal firewall shall be employed on all mobile devices that have a full-feature operating system (i.e. laptops or tablets with Windows or Linux/Unix operating systems). At a minimum, the personal firewall shall perform the following activities:

1. Manage program access to the Internet.
2. Block unsolicited requests to connect to the user device.
3. Filter incoming traffic by IP address or protocol.
4. Filter incoming traffic by destination ports.
5. Maintain an IP traffic log.

Mobile devices with limited-feature operating systems (i.e. tablets, smartphones) may not support a personal firewall. However, these operating systems have a limited number of system services installed, carefully controlled network access, and to a certain extent, perform functions similar to a personal firewall on a device with a full-feature operating system. Appropriately configured MDM software is capable of controlling which applications are allowed on the device. [Source: FBI CJIS CSP v5.9]

SUPPLEMENTAL GUIDANCE

Mobile code includes any program, application, or content that can be transmitted across a network (e.g., embedded in an email, document, or website) and executed on a remote system. Decisions regarding the use of mobile code within organizational systems are based on the potential for the code to cause damage to the systems if used maliciously. Mobile code technologies include Java applets, JavaScript, HTML5, WebGL, and VBScript. Usage restrictions and implementation guidelines apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices, including notebook computers and smart phones. Mobile code policy and procedures address specific actions taken to prevent the development, acquisition, and introduction of unacceptable mobile code within organizational systems, including requiring mobile code to be digitally signed by a trusted source.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FBI CJIS CSP v5.9.	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing mobile code; mobile code usage restrictions; mobile code implementation policy and procedures; system design documentation; system configuration settings and associated documentation; list of unacceptable mobile code; list of corrective actions to be taken when unacceptable mobile code is identified; system monitoring records; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with responsibilities for managing mobile code.

Test: Automated mechanisms supporting and/or implementing mobile code detection, inspection, and corrective capabilities.

SC-18(02): ACQUISITION / DEVELOPMENT / USE

Priority: P1

Baseline(s): N/A	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization ensures that the acquisition, development, and use of mobile code to be deployed in the information system meets DFPS-defined mobile code requirements.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - DFPS must document and define the mobile code technologies used in System Security Plans (SSPs).

Std.02 – The DFPS Chief Information Security Officer or their delegate reviews and approves System Security Plans (SSPs) on an annual basis.

SUPPLEMENTAL GUIDANCE

None.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** N/A **Federal**: FBI CJIS CSP v5.9.	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing mobile code; mobile code requirements; mobile code usage restrictions; mobile code implementation policy and procedures; acquisition documentation; acquisition contracts for system, system component, or system service; system development life cycle documentation; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with responsibilities for managing mobile code; organizational personnel with acquisition and contracting responsibilities.

Test: Organizational processes for the acquisition, development, and use of mobile code.

SC-18(03): PREVENT DOWNLOADING / EXECUTION

Priority: P1

Baseline(s): N/A	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization prevents the download and execution of non-approved or unacceptable mobile code.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Configure systems to prevent installation or execution of unapproved, unauthorized, or unmanaged mobile code in accordance with CA-07(04).

SUPPLEMENTAL GUIDANCE

None.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** N/A **Federal**: FBI CJIS CSP v5.9.	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing mobile code; mobile code usage restrictions; mobile code implementation policy and procedures; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with responsibilities for managing mobile code.

Test: Automated mechanisms preventing download and execution of unacceptable mobile code.

SC-18(04): PREVENT AUTOMATIC EXECUTION

Priority: P1	
Baseline(s): N/A	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization prevents the automatic execution of mobile code in organization-defined software applications and enforce organization-defined actions prior to executing the code.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - Detect the presence of unauthorized software and mobile code components within the system using automated mechanisms as identified in the System Security Plan (SSP) continuously in accordance with CM-08.

Std.02 - Disable network access by such components; isolate the components; and notify personnel as identified in the incident response plan in accordance with CM-08.

SUPPLEMENTAL GUIDANCE

Actions enforced before executing mobile code include prompting users prior to opening email attachments or clicking on web links. Preventing the automatic execution of mobile code includes disabling auto-execute features on system components that employ portable storage devices, such as compact discs, digital versatile discs, and universal serial bus devices.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** N/A **Federal**: FBI CJIS CSP v5.9.	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing mobile code; mobile code usage restrictions; mobile code implementation policy and procedures; system design documentation; system configuration settings and associated documentation; list of software applications in which the automatic execution of mobile code must be prohibited; list of actions required before execution of mobile code; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with responsibilities for managing mobile code.

Test: Automated mechanisms preventing the automatic execution of unacceptable mobile code; automated mechanisms enforcing actions to be taken prior to the execution of the mobile code.

SC-19: VOICE OVER INTERNET PROTOCOL

Priority: P1	
Baseline(s): N/A	Overlay(s): CJIS

CONTROL REQUIREMENTS

This control is withdrawn as technology-specific and addressed as any other technology or protocol, but still referenced in the FBI CJIS Security Policy v5.9.

SC-20: SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and

b. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Enable remote clients to obtain origin authentication and integrity verification assurances along with the authoritative data for the name/address resolution information obtained through the service consistent with the guidance in NIST SP 800-81.

a. Mechanisms to ensure that name/address resolution service provides additional data origin, integrity artifacts, and authoritative data in response to queries should include all of the following:
    1. Digital signatures;
    2. Digital certificates;
    3. Digital time stamping;
    4. DNSSEC;
    5. Approved encryption requirements and technology (see SC-13).
    6. Additionally, means to indicate the security status of child subspaces may include delegation signer (DS) resource records in the DNS.

SUPPLEMENTAL GUIDANCE

Providing authoritative source information enables external clients, including remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. Systems that provide name and address resolution services include domain name system (DNS) servers. Additional artifacts include DNS Security Extensions (DNSSEC) digital signatures and cryptographic keys. Authoritative data includes DNS resource records. The means for indicating the security status of child zones include the use of delegation signer resource records in the DNS. Systems that use technologies other than the DNS to map between host and service names and network addresses provide other means to assure the authenticity and integrity of response data.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy.	AU-10, SC-8, SC-12, SC-13, SC-21, SC-22.

State: DIR Security Control Standards Catalog. **Federal**: FIPS 140, 186; NIST SP 800-81-2; FBI CJIS CSP v5.9.	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing secure name/address resolution services (authoritative source); system design documentation; system configuration settings and associated documentation; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with responsibilities for managing DNS.

Test: Automated mechanisms supporting and/or implementing secure name/address resolution services.

SC-21: SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — The information system that provides name/address resolution service for local clients must perform data origin authentication and data integrity verification on the resolution responses it receives from authoritative sources when requested by client systems following the guidance in NIST SP 800-81, Security Domain Name Deployment Guide. [Source: DIR Control Standards Catalog SC-21]

SUPPLEMENTAL GUIDANCE

Each client of name resolution services either performs this validation on its own or has authenticated channels to trusted validation providers. Information systems that provide name and address resolution services for local clients include, for example, recursive resolving or caching domain name system (DNS) servers. DNS client resolvers either perform validation of DNSSEC signatures, or clients use authenticated channels to recursive resolvers that perform such validations. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to enable clients to verify the authenticity and integrity of response data.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: NIST SP 800-81-2; FBI CJIS CSP v5.9.	SC-20, SC-22.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing secure name/address resolution services (recursive or caching resolver); system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with responsibilities for managing DNS.

Test: Automated mechanisms supporting and/or implementing data origin authentication and data integrity verification for name/address resolution services.

SC-22: ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Systems that provide name and address resolution services include domain name system (DNS) servers. To eliminate single points of failure in systems and enhance redundancy, organizations employ at least two authoritative domain name system servers—one configured as the primary server and the other configured as the secondary server.

Additionally, organizations typically deploy the servers in two geographically separated network subnetworks (i.e., not located in the same physical facility). For role separation, DNS servers with internal roles only process name and address resolution requests from within organizations (i.e., from internal clients). DNS servers with external roles only process name and address resolution information requests from clients external to organizations (i.e., on external networks, including the Internet). Organizations specify clients that can access authoritative DNS servers in certain roles (e.g., by address ranges and explicit lists).

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: NIST SP 800-81-2; FBI CJIS CSP v5.9.	SC-2, SC-20, SC-21, SC-24.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing architecture and provisioning for name/address resolution services; access control policy and procedures; system design documentation; assessment results from independent testing organizations; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with responsibilities for managing DNS.

Test: Automated mechanisms supporting and/or implementing name/address resolution services for fault tolerance and role separation.

SC-23: SESSION AUTHENTICITY

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The information system protects the authenticity of communications sessions.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Provide session-level protection using approved cryptographic modules in accordance with SC-13.

SUPPLEMENTAL GUIDANCE

Protecting session authenticity addresses communications protection at the session level, not at the packet level. Such protection establishes grounds for confidence at both ends of communications sessions in the ongoing identities of other parties and the validity of transmitted information. Authenticity protection includes protecting against "man-in-the- middle" attacks, session hijacking, and the insertion of false information into sessions.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: NIST SP 800-52, 800-77, 800-95, 800-113; FBI CJIS CSP v5.9.	AU-10, SC-8, SC-10, SC-11.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing session authenticity; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities.

Test: Automated mechanisms supporting and/or implementing session authenticity.

SC-23(01): INVALIDATE SESSION IDENTIFIERS AT LOGOUT

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The information system invalidates session identifiers upon user logout or other session termination.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Invalidating session identifiers at logout curtails the ability of adversaries to capture and continue to employ previously valid session IDs.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FBI CJIS CSP v5.9.	None.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing session authenticity; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities.

Test: Automated mechanisms supporting and/or implementing session identifier invalidation upon session termination.

SC-23(03): UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The information system generates a unique session identifier for each session with randomness defined in the system security plan (SSP) and recognize only session identifiers that are system-generated.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Generating unique session identifiers curtails the ability of adversaries to reuse previously valid session IDs. Employing the concept of randomness in the generation of unique session identifiers protects against brute-force attacks to determine future session identifiers.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FBI CJIS CSP v5.9.	AC-10, SC-12, SC-13.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing session authenticity; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities.

Test: Automated mechanisms supporting, implementing, generating, and monitoring unique session identifiers; automated mechanisms supporting and/or implementing randomness requirements.

SC-24: FAIL IN KNOWN STATE

Priority: P1

Baseline(s): High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The information system fails to a known secure state for the following failures on the indicated components while preserving system state information as defined in Std.01 in failure: all types of system failures on system components under configuration management.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Configure systems to preserve state information necessary to:

a. Determine cause of failure;
b. Return to operations with least disruption to mission and business processes; and
c. Permit investigations of failure.
d. Information preserved in failure should include state variables and whether communication is permitted or blocked.

SUPPLEMENTAL GUIDANCE

Failure in a known state addresses security concerns in accordance with the mission/business needs of organizations. Failure in a known secure state helps to prevent the loss of confidentiality, integrity, or availability of information in the event of failures of organizational information systems or system components. Failure in a known safe state helps to prevent systems from failing to a state that may cause injury to individuals or destruction to property. Preserving information system state information facilitates system restart and return to the operational mode of organizations with less disruption of mission/business processes.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FBI CJIS CSP v5.9.	CP-2, CP-4, CP-10, CP-12, SA-8, SC-7, SC-22, SI-13.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing session authenticity; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities.

Test: Automated mechanisms supporting, implementing, generating, and monitoring unique session identifiers; automated mechanisms supporting and/or implementing randomness requirements.

SC-26: DECOYS

Priority: P0

Baseline(s): N/A	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization includes components within organizational systems specifically designed to be the target of malicious attacks for detecting, deflecting, and analyzing such attacks

AGENCY IMPLEMENTATION STANDARDS

Std.01 – The DFPS Office of Information Security may utilize decoys as part of the Information Security Program and control PM-01.

SUPPLEMENTAL GUIDANCE

Decoys (i.e., honeypots, honeynets, or deception nets) are established to attract adversaries and deflect attacks away from the operational systems that support organizational mission and business functions. Use of decoys requires some supporting isolation measures to ensure that any deflected malicious code does not infect organizational systems. Depending on the specific usage of the decoy, consultation with the Office of the General Counsel before deployment may be needed.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FBI CJIS CSP v5.9.	RA-5, SC-7, SC-30, SC-35, SC-44, SI-3, SI-4.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing the use of decoys; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; system developer.

Test Automated mechanisms supporting and/or implementing decoys.

SC-28: PROTECTION OF INFORMATION AT REST

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The information system protects the confidentiality and integrity of the following information at rest: DFPS data classified as Sensitive, Confidential, or Controlled.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — All DFPS data classified as Sensitive, Confidential, or Regulated must be encrypted at rest using an encryption algorithm compliant with SC-13 and SC-28(01).

For systems processing CJIS data, or that support CJIS processes, the following additional Implementation Standard applies:

Std.02 - When encryption is employed, agencies shall either encrypt CJI in accordance with the standard in Section 5.10.1.2.1 of the FBI CJIS Security Policy, or use a symmetric cipher that is FIPS 197 certified (AES) and at least 256 bit strength.

1. When agencies implement encryption on CJI at rest, the passphrase used to unlock the cipher shall meet the following requirements:
   a. Be at least 10 characters
   b. Not be a dictionary word.
   c. Include at least one (1) upper case letter, one (1) lower case letter, one (1) number, and one (1) special character.
   d. Be changed when previously authorized personnel no longer require access.
2. Multiple files maintained in the same unencrypted folder shall have separate and distinct passphrases. A single passphrase may be used to encrypt an entire folder or disk containing multiple files. All audit requirements found in Section 5.4.1 Auditable Events and Content (Information Systems) shall be applied.

NOTE: Commonly available encryption tools often use a key to unlock the cipher to allow data access; this key is called a passphrase. While similar to a password, a passphrase is not used for user authentication. Additionally, the passphrase contains stringent character requirements making it more secure and thus providing a higher level of confidence that the passphrase will not be compromised. [Source: FBI CJIS Security Policy]

SUPPLEMENTAL GUIDANCE

Information at rest refers to the state of information when it is not in process or in transit and is located on system components. Such components include internal or external hard disk drives, storage area network devices, or databases. However, the focus of protecting information at rest is not on the type of storage device or frequency of access but rather on the state of the information. Information at rest addresses the confidentiality and integrity of information and covers user information and system information. System-related information that requires protection includes configurations or rule sets for firewalls, intrusion detection and prevention systems, filtering routers, and authentication information. Organizations may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms and file share scanning. Integrity protection can be achieved, for example, by implementing write-once-read-many (WORM) technologies. When adequate protection of information at rest cannot otherwise be achieved, organizations may employ other controls, including frequent scanning to identify malicious code at rest and secure offline storage in lieu of online storage.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; NIST SP 800-56A, 800-56B, 800-56C, 800-57-1, 800-57-2, 800-57-3, 800-111, 800-124; FBI CJIS CSP v5.9.	AC-3, AC-4, AC-6, AC-19, CA-7, CM-3, CM-5, CM-6, CP-9, MP-4, MP-5, PE-3, SC-8, SC-12, SC-13, SC-34, SI-3, SI-7, SI-16.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing the protection of information at rest; system design documentation; system configuration settings and associated documentation; cryptographic mechanisms and associated configuration documentation; list of information at rest requiring confidentiality and integrity protections; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; system developer.

Test: Automated mechanisms supporting and/or implementing confidentiality and integrity protections for information at rest.

SC-28(01): CRYPTOGRAPHIC PROTECTION

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on all digital media: DFPS data classified as Sensitive, Confidential, or Controlled.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Implement encryption algorithms in accordance with SC-13.

SUPPLEMENTAL GUIDANCE

Selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of organizational information. The strength of mechanism is commensurate with the security category and/or classification of the information. This control enhancement applies to significant concentrations of digital media in organizational areas designated for media storage and also to limited quantities of media generally associated with information system components in operational environments (e.g., portable storage devices, mobile devices). Organizations have the flexibility to either encrypt all information on storage devices (i.e., full disk encryption) or encrypt specific data structures (e.g., files, records, or fields). Organizations employing cryptographic mechanisms to protect information at rest also consider cryptographic key management solutions.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; NIST SP 800-56A, 800-56B, 800-56C, 800-57-1, 800-57-2, 800-57-3, 800-111, 800-124; FBI CJIS CSP v5.9.	AC-19, SC-12, SC-13.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing the protection of information at rest; system design documentation; system configuration settings and associated documentation; cryptographic mechanisms and associated configuration documentation; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; system developer.

Test: Cryptographic mechanisms implementing confidentiality and integrity protections for information at rest.

SC-28(02): OFFLINE STORAGE

Priority: P1

Baseline(s): N/A	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization remove the following information from online storage and store offline in a secure location: CJIS Information

AGENCY IMPLEMENTATION STANDARDS

Std.01 — When CJI is at rest (i.e. stored digitally) outside the boundary of the physically secure location, the data shall be protected via encryption.

a. When encryption in transit is employed, the cryptographic module used shall be FIPS 140-2 certified and use a symmetric cipher key strength of at least 128 bit strength to protect CJI.

b. When encryption ast rest is employed, agencies shall encrypt CJI with a symmetric cipher that is FIPS 197 certified (AES) and at least 256 bit strength.

SUPPLEMENTAL GUIDANCE

Removing organizational information from online information system storage to off-line storage eliminates the possibility of individuals gaining unauthorized access to the information through a network. Therefore, organizations may choose to move information to off-line storage in lieu of protecting such information in online storage.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FBI CJIS CSP v5.9.	None.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing the protection of information at rest; system design documentation; system configuration settings and associated documentation; cryptographic mechanisms and associated configuration documentation; offline storage locations for information at rest; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities.

Test: Automated mechanisms supporting and/or implementing the removal of information from online storage; automated mechanisms supporting and/or implementing storage of information offline.

SC-32: SYSTEM PARTITIONING

Priority: P0

Baseline(s): N/A	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization partitions the information system into defined information system components (defined in the applicable System Security Plan [SSP]) residing in separate physical domains or environments based on defined circumstances (defined in the applicable SSP) for physical separation of components.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - The application, service, or information system shall separate user functionality (including user interface services) from information system management functionality. [Source: FBI CJIS Security Policy]

Std.02 -The application, service, or information system shall physically or logically separate user interface services (e.g. public web pages) from information storage and management services (e.g. database management). Separation may be accomplished through the use of one or more of the following:

a. Different computers.
b. Different central processing units.
c. Different instances of the operating system.
d. Different network addresses.
e. Other methods approved by the DPS CJIS CISO.

[Source: FBI CJIS Security Policy]

SUPPLEMENTAL GUIDANCE

Information system partitioning is a part of a defense-in-depth protection strategy. Organizations determine the degree of physical separation of system components from physically distinct components in separate racks in the same room, to components in separate rooms for the more critical components, to more significant geographical separation of the most critical components. Security categorization can guide the selection of appropriate candidates for domain partitioning. Managed interfaces restrict or prohibit network access and information flow among partitioned information system components.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FBI CJIS CSP v5.9.	AC-4, AC-6, SA-8, SC-2, SC-3, SC-7, SC-36.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing system partitioning; system design documentation; system configuration settings and associated documentation; system architecture; list of system physical domains (or environments); system facility diagrams; system network diagrams; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; system developers/integrators.

Test: Automated mechanisms supporting and/or implementing the physical separation of system components.

SC-36: DISTRIBUTED PROCESSING AND STORAGE

Priority: P0

Baseline(s): N/A	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization distributes, for cloud computing of CJIS information, processing, and storage across multiple physical locations.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - The storage of CJI, regardless of encryption status, shall only be permitted in cloud environments (e.g. government or third-party/commercial datacenters, etc.) which reside within the physical boundaries of APB-member country (i.e. U.S., U.S. territories, Indian Tribes, and Canada) and legal authority of an APB-member agency (i.e. U.S. – federal/state/territory, Indian Tribe, or the Royal Canadian Mounted Police (RCMP)).

Note: This restriction does not apply to exchanges of CJI with foreign government agencies under international exchange agreements (i.e. the Preventing and Combating Serious Crime (PCSC) agreements, fugitive extracts, and exchanges made for humanitarian and criminal investigatory purposes in particular circumstances). [Source: FBI CJIS Security Policy]

Std.02 - Metadata derived from unencrypted CJI shall be protected in the same manner as CJI and shall not be used for any advertising or other commercial purposes by any cloud service provider or other associated entity.

Note: The agency may permit limited use of metadata derived from unencrypted CJI when specifically approved by the agency and its "intended use" is detailed within the service agreement. Such authorized uses of metadata may include, but are not limited to the following: spam and spyware filtering, data loss prevention, spillage reporting, transaction logs (events and content – similar to Section 5.4), data usage/indexing metrics, and diagnostic/syslog data. [Source: FBI CJIS Security Policy]

SUPPLEMENTAL GUIDANCE

Distributing processing and storage across multiple physical locations provides some degree of redundancy or overlap for organizations, and therefore increases the work factor of adversaries to adversely impact organizational operations, assets, and individuals. This control does not assume a single primary processing or storage location, and thus allows for parallel processing and storage.

REFERENCES	RELATED CONTROLS

Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: NIST 800-144, 800- 145, and 800-146; FBI CJIS CSP v5.9.	CP-6, CP-7, PL-8, SC-32.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; contingency planning policy and procedures; contingency plan; system design documentation; system configuration settings and associated documentation; system architecture; list of system physical locations (or environments) with distributed processing and storage; system facility diagrams; processing site agreements; storage site agreements; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel with contingency planning and plan implementation responsibilities; system developers/integrators.

Test: Organizational processes for distributed processing and storage across multiple physical locations; automated mechanisms supporting and/or implementing the capability to distribute processing and storage across multiple physical locations.

SC-37: OUT-OF-BAND CHANNELS

Priority: P0

Baseline(s): N/A	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization employs FBI defined out-of-band channels for the physical delivery or electronic transmission of information, information system components, or devices to individuals or information systems that process CJIS.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - One-time passwords are considered a "something you have" token for authentication. Examples include bingo cards, hard or soft tokens, and out-of-band tokens (i.e. OTP received via a text message).

When agencies implement the use of an OTP as an authenticator, the OTP shall meet the requirements described below.

1. Be a minimum of six (6) randomly generated characters
2. Be valid for a single session
3. If not used, expire within a maximum of five (5) minutes after issuance [Source: FBI CJIS Security Policy]

SUPPLEMENTAL GUIDANCE

Distributing processing and storage across multiple physical locations provides some degree of redundancy or overlap for organizations, and therefore increases the work factor of adversaries to adversely impact organizational operations, assets, and individuals. This control does not assume a single primary processing or storage location, and thus allows for parallel processing and storage.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: NIST 800-144, 800- 145, and 800-146; FBI CJIS CSP v5.9.	CP-6, CP-7, PL-8, SC-32.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing the use of out-of-band channels; access control policy and procedures; identification and authentication policy and procedures; system design documentation; system architecture; system configuration settings and associated documentation; list of out-of-band channels; types of information, system components, or devices requiring the use of out-of-band channels for physical delivery or electronic transmission to authorized individuals or systems; physical delivery records; electronic transmission records; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel authorizing, installing, configuring, operating, and/or using out-of-band channels; system developers/integrators.

Test: Organizational processes for the use of out-of-band channels; automated mechanisms supporting and/or implementing the use of out-of-band channels.

SC-37(01): ENSURE DELIVERY AND TRANSMISSION

Priority: P0

Baseline(s): N/A	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization employs FBI defined security safeguards to ensure that only authorized individuals or information systems receive the CJIS information, information system components, or devices.

AGENCY IMPLEMENTATION STANDARDS

Std.01 – When accessing CJI from an authorized mobile device, Advanced Authentication (AA) shall be used by the authorized user. When certificates or cryptographic keys used to authenticate a mobile device, they shall be:

1. Protected against being extracted from the device.
2. Configured for remote wipe on demand or self-deletion based on a number of unsuccessful login or access attempts
3. Configured to use a secure authenticator (i.e. password, PIN) to unlock the key for use. [Source: FBI CJIS Security Policy]

Std.02 - Advanced Authentication (AA) provides for additional security to the typical user identification and authentication of login ID and password, such as: biometric systems, user-based digital certificates (e.g. public key infrastructure (PKI)), smart cards, software tokens, hardware tokens, paper (inert) tokens, out-of-band authenticators (retrieved via a separate communication service channel – e.g., authenticator is sent on demand via text message, phone call, etc.), or "Risk-based Authentication" that includes a software token element comprised of a number of factors, such as network information, user information, positive device identification (i.e. device forensics, user pattern analysis and user binding), user profiling, and high-risk challenge/response questions.

When user-based certificates are used for authentication purposes, they shall:

1. Be specific to an individual user and not to a particular device.
2. Prohibit multiple users from utilizing the same certificate.
3. Require the user to "activate" that certificate for each use in some manner (e.g., passphrase or user-specific PIN). [Source: FBI CJIS Security Policy]

SUPPLEMENTAL GUIDANCE

Techniques and/or methods employed by organizations to ensure that only designated information systems or individuals receive particular information, system components, or devices include, for example, sending authenticators via courier service but requiring recipients to show some form of government-issued photographic identification as a condition of receipt.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FBI CJIS CSP v5.9.	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing the use of out-of-band channels; access control policy and procedures; identification and authentication policy and procedures; system design documentation; system architecture; system configuration settings and associated documentation; list of security safeguards to be employed to ensure that designated individuals or systems receive organization-defined information, system components, or devices; list of security safeguards for delivering designated information, system components, or devices to designated individuals or systems; list of information, system components, or devices to be delivered to designated individuals or systems; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel authorizing, installing, configuring, operating, and/or using out-of-band channels; system developers/integrators.

Test: Organizational processes for the use of out-of-band channels; automated mechanisms supporting and/or implementing the use of out-of-band channels; automated mechanisms supporting/implementing safeguards to ensure delivery of designated information, system components, or devices.

SC-38: OPERATIONS SECURITY

Priority: P0

Baseline(s): N/A	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization employs operations security safeguards to protect key organizational information throughout the system development life cycle in accordance with the FBI CJIS Security Policy.

AGENCY IMPLEMENTATION STANDARDS

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.01 – FBI defined operations security safeguards should be documented in the system security plan (SSP) and approved by the DFPS Chief Information Security Officer (CISO).

SUPPLEMENTAL GUIDANCE

Operations security (OPSEC) is a systematic process by which potential adversaries can be denied information about the capabilities and intentions of organizations by identifying, controlling, and protecting generally unclassified information that specifically relates to the planning and execution of sensitive organizational activities. The OPSEC process involves five steps: (i) identification of critical information (e.g., the security categorization process); (ii) analysis of threats; (iii) analysis of vulnerabilities; (iv) assessment of risks; and (v) the application of appropriate countermeasures. OPSEC safeguards are applied to both organizational information systems and the environments in which those systems operate. OPSEC safeguards help to protect the confidentiality of key information including, for example, limiting the sharing of information with suppliers and potential suppliers of information system components, information technology products and services, and with other non-organizational elements and individuals. Information critical to mission/business success includes, for example, user identities, element uses, suppliers, supply chain processes, functional and security requirements, system design specifications, testing protocols, and security control implementation details.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FBI CJIS CSP v5.9.	CA-2, CA-7, PL-1, PM-9, PM-12, RA-2, RA-3, RA-5, SC-7, SR-3, SR-7.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing operations security; security plan; list of operations security safeguards; security control assessments; risk assessments; threat and vulnerability assessments; plans of action and milestones; system development life cycle documentation; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; system developers/integrators.

Test: Organizational processes for protecting organizational information throughout the system development life cycle; automated mechanisms supporting and/or implementing safeguards to protect organizational information throughout the system development life cycle.

SC-39: PROCESS ISOLATION

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The information system maintains a separate execution domain for each executing process.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Use operating systems that support process isolation. [Source: DIR Control Standards Catalog SC-39]

SUPPLEMENTAL GUIDANCE

Systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each system process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process.

Maintaining separate execution domains for executing processes can be achieved, for example, by implementing separate address spaces. Process isolation technologies, including sandboxing or virtualization, logically separate software and firmware from other software, firmware, and data. Process isolation helps limit the access of potentially untrusted software to other system resources. The capability to maintain separate execution domains is available in commercial operating systems that employ multi-state processor technologies.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: NIST SP 800-160-1; FBI CJIS CSP v5.9.	AC-3, AC-4, AC-6, AC-25, SA-8, SC-2, SC-3, SI-16.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System design documentation; system architecture; independent verification and validation documentation; testing and evaluation documentation; other relevant documents or records.

Interview: System developers/integrators; system security architect

Test: Automated mechanisms supporting and/or implementing separate execution domains for each executing process

SC-40: WIRELESS LINK PROTECTION

Priority: P0

Baseline(s): N/A	Overlay(s): CJIS

CONTROL REQUIREMENTS

The information system protects external and internal wireless links that process CJI from the requirements outlined in Std.1.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — When an agency allows mobile devices that are approved to access or store CJI to function as a Wi-Fi hotspot connecting to the Internet, they shall be configured:

a. Enable encryption on the hotspot;
b. Change the hotspot's default SSID;
c. Ensure the hotspot SSID does not identify the device make/model or agency ownership;
d. Create a wireless network password (Pre-shared key);
e. Enable the hotspot's port filtering/blocking features if present;
f. Only allow connections from agency controlled devices.

Note: Refer to the requirements in the FBI CJIS Security Policy Section 5.10.1.2 encryption for item #1. Refer to the requirements in Section 5.6.2.2.1 Password for item #3. Only password attributes #1, #2 and #3 are required.

OR

1. Have a MDM solution to provide the same security as identified in items 1 – 5 above. [Source: FBI CJIS Security Policy]

SUPPLEMENTAL GUIDANCE

Wireless link protection applies to internal and external wireless communication links that may be visible to individuals who are not authorized system users. Adversaries can exploit the signal parameters of wireless links if such links are not adequately protected. There are many ways to exploit the signal parameters of wireless links to gain intelligence, deny service, or spoof system users. Protection of wireless links reduces the impact of attacks that are unique to wireless systems. If organizations rely on commercial service providers for transmission services as commodity items rather than as fully dedicated services, it may not be possible to implement wireless link protections to the extent necessary to meet organizational security requirements.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: NIST SP 800-160-1; FBI CJIS CSP v5.9.	AC-18, SC-5.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; access control policy and procedures; procedures addressing wireless link protection; system design documentation; wireless network diagrams; system configuration settings and associated documentation; system architecture; list of internal and external wireless links; list of signal parameter attacks or references to sources for attacks; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel authorizing, installing, configuring, and/or maintaining internal and external wireless links.

Test: Automated mechanisms supporting and/or implementing protection of wireless links.

SC-43: USAGE RESTRICTIONS

Priority: P0

Baseline(s): N/A	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization:

a. Establishes usage restrictions and implementation guidance for CJI information stored or process in a cloud environment based on the potential to cause damage to the information system if used maliciously; and

b. Authorizes, monitors, and controls the use of such components within the information system.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — CJI may not be used in cloud-based enviroments unless explicitly approved by the DFPS Chief Information Security Officer.

Std.01 — FBI defined operations security safeguards for cloud computing should be documented in the system security plan (SSP) and approved by the DFPS Chief Information Security Officer (CISO).

SUPPLEMENTAL GUIDANCE

Information system components include hardware, software, or firmware components (e.g., Voice Over Internet Protocol, mobile code, digital copiers, printers, scanners, optical devices, wireless technologies, mobile devices).

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FBI CJIS CSP v5.9.	AC-18, AC-19, CM-6, SC-7, SC-18.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; usage restrictions; procedures addressing usage restrictions; implementation policy and procedures; authorization records; system monitoring records; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system.

Test: Organizational processes for authorizing, monitoring, and controlling the use of components with usage restrictions; Automated mechanisms supporting and/or implementing, authorizing, monitoring, and controlling the use of components with usage restrictions.

SC-44: DETONATION CHAMBERS

Priority: P0

Baseline(s): N/A	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization employs a detonation chamber capability within a defined system, system component, or location.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — The DFPS Office of Information security utilizes detonation chambers to execute untrusted or suspicious applications, execute Universal Resource Locator (URL) requests in the safety of an isolated environment or a virtualized sandbox.

SUPPLEMENTAL GUIDANCE

Detonation chambers, also known as dynamic execution environments, allow organizations to open email attachments, execute untrusted or suspicious applications, and execute Universal Resource Locator requests in the safety of an isolated environment or a virtualized sandbox. Protected and isolated execution environments provide a means of determining whether the associated attachments or applications contain malicious code. While related to the concept of deception nets, the employment of detonation chambers is not intended to maintain a long-term environment in which adversaries can operate and their actions can be observed. Rather, detonation chambers are intended to quickly identify malicious code and either reduce the likelihood that the code is propagated to user environments of operation or prevent such propagation completely.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FBI CJIS CSP v5.9.	AC-18, AC-19, CM-6, SC-7, SC-18.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; usage restrictions; procedures addressing usage restrictions; implementation policy and procedures; authorization records; system monitoring records; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system.

Test: Organizational processes for authorizing, monitoring, and controlling the use of components with usage restrictions; Automated mechanisms supporting and/or implementing, authorizing, monitoring, and controlling the use of components with usage restrictions.

SC-45: SYSTEM TIME SYNCHRONIZATION

Priority: P0

Baseline(s): N/A	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization synchronize system clocks within and between systems and system components.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Ensure that system clocks meet the degree of synchronization in accordance with AU-08.

SUPPLEMENTAL GUIDANCE

Time synchronization of system clocks is essential for the correct execution of many system services, including identification and authentication processes that involve certificates and time-of-day restrictions as part of access control. Denial of service or failure to deny expired credentials may result without properly synchronized clocks within and between systems and system components. Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. The granularity of time measurements refers to the degree of synchronization between system clocks and reference clocks, such as clocks synchronizing within hundreds of milliseconds or tens of milliseconds. Organizations may define different time granularities for system components. Time service can be critical to other security capabilities—such as access control and identification and authentication—depending on the nature of the mechanisms used to support the capabilities.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: IETF 5905	AC-3, AU-8, IA-2, IA-8.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing time synchronization; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system.

Test: Automated mechanisms supporting and/or implementing system time synchronization.

SC-45(01): SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE

Priority: P0

Baseline(s): N/A	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization:

a. Compare the internal system clocks at least once daily and at system boot with an approved authoritative time source as defined in Std.01; and

b. Synchronize the internal system clocks to the authoritative time source when the time difference is greater than the granularity defined in AU-08.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Configure internal system clocks to synchronize with an agency approved, authoritative source.

SUPPLEMENTAL GUIDANCE

Synchronization of internal system clocks with an authoritative source provides uniformity of time stamps for systems with multiple system clocks and systems connected over a network.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: IETF 5905.	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing time synchronization; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or record.

Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system.

Test: Automated mechanisms supporting and/or implementing system time synchronization.

(SI) SYSTEM AND INFORMATION INTEGRITY

DFPS provides oversight to ensure controls are in place that protect system and information integrity. These controls include flaw remediation, malicious code protection, information system monitoring, security alerts, software and firmware integrity, and spam protection.

The intended audience for this Control includes, but is not limited to, information resource owners and custodians. The information resource owner, or their designee, is responsible for ensuring that system and integrity measures described in this Control family are implemented by personnel with system and integrity responsibilities (e.g. system/network administrators, information security analyst, etc.).

SI-01: SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization:

a. Develop, document, and disseminate to appropriate personnel:
   2. Organization-level system and information integrity policy that:
      a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   3. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;
b. Designate a senior management official as defined in the system and information integrity policy to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; and
c. Review and update the current system and information integrity:
   1. Policy every two (2) years and following major changes to legislation or security requirements; and
   2. Procedures every two (2) years and following major changes to legislation or security requirements.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — The integrity of data, its source, its destination, and processes applied to it shall be assured. Changes to data shall be made only in an authorized manner. [Source: DIR Control Standards Catalog SI-1]

Std.02 — The DFPS Chief Information Security Officer shall be responsible for:

a. Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks;

b. Providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities under 1 TAC 202; and

c. Developing and recommending policies and establishing procedures and practices, in cooperation with the agency Information Resources Manager, information-owners and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, or disclosure. [Source: 1 TAC 202.21(b)(3, 5, 8)]

SUPPLEMENTAL GUIDANCE

System and information integrity policy and procedures address the controls in the SI family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of system and information integrity policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to system and information integrity policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; NIST SP 800-12, 800-100.	PM-9, PS-8, SA-8, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy; system and information integrity procedures; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with system and information integrity responsibilities; organizational personnel with information security and privacy responsibilities,

SI-02: FLAW REMEDIATION

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Identify, report, and correct system flaws;

b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

c. Install security-relevant software and firmware updates within time periods defined in accordance with RA-05 Std.07 of the release of the updates; and

d. Incorporate flaw remediation into the organizational configuration management process.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS must identify, report, and correct information system flaws. [Source: DIR Control Standards Catalog SI-2]

Std.02 —

a. DFPS shall, with available funds, identify information security issues and develop a plan to prioritize the remediation and mitigation of those issues. DFPS shall include in the plan:

    1. Procedures for reducing the agency's level of exposure with regard to information that alone or in conjunction with other information identifies an individual maintained on a legacy system of the agency;

    2. The best value approach for modernizing, replacing, renewing, or disposing of a legacy system that maintains information critical to the agency's responsibilities;

b. A plan developed under this section, along with any information or communication prepared or maintained for use in the preparation of the plan, is confidential and is not subject to disclosure under Chapter 552. [Source: TX Govt. Code 2054.575]

Std.03 — Review available published sources and alerts identifying software flaws.

Std.04 — Where feasible, test newly released security relevant patches, service packs, and hot fixes in a test environment.

Std.05 — Patches, service packs, and hot fixes not implemented in enterprise or specific systems must be documented in the risk register.

Std.06 — Monitor systems to verify that security releases have been installed and are functioning correctly.

SUPPLEMENTAL GUIDANCE

The need to remediate system flaws applies to all types of software and firmware. Organizations identify systems affected by software flaws, including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security and privacy responsibilities. Security-relevant updates include patches, service packs, and malicious code signatures. Organizations also address flaws discovered during assessments, continuous monitoring, incident response activities, and system error handling. By incorporating flaw remediation into configuration management processes, required remediation actions can be tracked and verified.

Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of risk factors, including the security category of the system, the criticality of the update (i.e., severity of

the vulnerability related to the discovered flaw), the organizational risk tolerance, the mission supported by the system, or the threat environment. Some types of flaw remediation may require more testing than other types.

Organizations determine the type of testing needed for the specific type of flaw remediation activity under consideration and the types of changes that are to be configuration managed. In some situations, organizations may determine that the testing of software or firmware updates is not necessary or practical, such as when implementing simple malicious code signature updates. In testing decisions, organizations consider whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** TX Govt. Code 2054.575; DIR Security Control Standards Catalog. **Federal**: OMB A-130; FIPS 140, 186; NIST SP 800-39, 800-40, 800-128; NIST IR 7788; FBI CJIS CSP v5.9.	CA-5, CM-3, CM-4, CM-5, CM-6, CM-8, MA-2, RA-5, SA-8, SA-10, SA-11, SI-3, SI-5, SI-7, SI-11.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy; system and information integrity procedures; procedures addressing flaw remediation; procedures addressing configuration management; list of flaws and vulnerabilities potentially affecting the system; list of recent security flaw remediation actions performed on the system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct system flaws); test results from the installation of software and firmware updates to correct system flaws; installation/change control records for security-relevant software and firmware updates; system security plan; privacy plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security and privacy responsibilities; organizational personnel responsible for installing, configuring, and/or maintaining the system; organizational personnel responsible for flaw remediation; organizational personnel with configuration management responsibilities.

Test: Organizational processes for identifying, reporting, and correcting system flaws; organizational process for installing software and firmware updates; automated mechanisms supporting and/or implementing the reporting and correcting of system flaws; automated mechanisms supporting and/or implementing testing software and firmware updates.

SI-02(02): AUTOMATED FLAW REMEDIATION STATUS

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization determines if system components have applicable security-relevant software and firmware updates installed using automated mechanisms where feasible at least once per quarter and on demand.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Where feasible, select remediation tools that include automated verification of remediation, or configure systems to automatically review files or configuration settings after remediation and mitigation activities.

Std.02 — Verification of remediation, whether automated or manual, must not employ exploit procedures (for example, penetration tests) or exploit codes without prior authorization and approval from the system's Authorizing Official (AO).

Std.03 — When flaw remediation and vulnerability mitigations are completed, update the system and component inventory to reflect current software versions and configurations.

SUPPLEMENTAL GUIDANCE

Automated mechanisms can track and determine the status of known flaws for system components.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** TX Govt. Code 2054.575; DIR Security Control Standards Catalog. **Federal**: OMB A-130; FIPS 140, 186; NIST SP 800-39, 800-40, 800-128; NIST IR 7788; FBI CJIS CSP v5.9.	CA-7, SI-4.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy; system and information integrity procedures; procedures addressing flaw remediation; automated mechanisms supporting centralized management of flaw remediation; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for flaw remediation.

Test: Automated mechanisms used to determine the state of system components with regard to flaw remediation.

SI-02(03): BENCHMARKS FOR CORRECTIVE ACTIONS

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization:

a. Measures the time between flaw identification and flaw remediation; and

b. Corrective actions must be taken within the time periods defined under the SI-2 (Flaw Remediation) Implementation Standards.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Organizations determine the time it takes on average to correct system flaws after such flaws have been identified and subsequently establish organizational benchmarks (i.e., time frames) for taking corrective actions. Benchmarks can be established by the type of flaw or the severity of the potential vulnerability if the flaw can be exploited.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** TX Govt. Code 2054.575; DIR Security Control Standards Catalog. **Federal**: OMB A-130; FIPS 140, 186; NIST SP 800-39, 800-40, 800-128; NIST IR 7788; FBI CJIS CSP v5.9.	None.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy; system and information integrity procedures; procedures addressing flaw remediation; system design documentation; system configuration settings and associated documentation; list of benchmarks for taking corrective action on identified flaws; records that provide timestamps of flaw identification and subsequent flaw remediation activities; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for flaw remediation.

Test: Organizational processes for identifying, reporting, and correcting system flaws; automated mechanisms used to measure the time between flaw identification and flaw remediation.

SI-03: MALICIOUS CODE PROTECTION

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Implement signature based, non-signature based, or both types of malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;

b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;

c. Configure malicious code protection mechanisms to:

   1. Perform periodic scans of the system at least daily and real-time scans of files from external sources at endpoints and network entry and exit points as the files are downloaded, opened, or executed in accordance with organizational policy; and

   2. Block and quarantine malicious code and send alert to administrators in response to malicious code detection; and

d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — The information system must implement malicious code protection. [Source: DIR Control Standards Catalog SI-3]

Std.02 — Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.

Std.03—Deploy anti-virus software on all systems commonly affected by malicious software (i.e. computers and servers).

Std.04 — Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.

Std.05 — For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.

Std.06 — Ensure that all anti-virus mechanisms are maintained as follows:

a. Are kept current;
b. Perform periodic scans; and
c. Generate audit logs which are retained to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. [Source: SP 800-171 3.3.1]

Std.07 — Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.

SUPPLEMENTAL GUIDANCE

System entry and exit points include firewalls, remote access servers, workstations, electronic mail servers, web servers, proxy servers, notebook computers, and mobile devices. Malicious code includes viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats contained within compressed or hidden files or hidden in files using techniques such as steganography. Malicious code can be inserted into systems in a variety of ways, including by electronic mail, the world-wide web, and portable storage devices. Malicious code insertions occur through the exploitation of system vulnerabilities. A variety of technologies and methods exist to limit or eliminate the effects of malicious code.

Malicious code protection mechanisms include both signature and non-signature-based technologies. non-signature-based detection mechanisms include artificial intelligence techniques that use heuristics to detect, analyze, and describe the characteristics or behavior of malicious code and to provide controls against such code for which signatures do not yet exist or for which existing signatures may not be effective. Malicious code for which active signatures do not yet exist or may be ineffective includes polymorphic malicious code (i.e., code that changes signatures when it replicates). Non-signature-based mechanisms also include reputation-based technologies. In addition to the above technologies, pervasive configuration management, comprehensive software integrity controls, and anti-exploitation software may be effective in preventing the execution of unauthorized code. Malicious code may be present in commercial off-the-shelf software as well as custom-built

software and could include logic bombs, backdoors, and other types of attacks that could affect organizational mission and business functions.

In situations where malicious code cannot be detected by detection methods or technologies, organizations rely on other types of controls, including secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to ensure that software does not perform functions other than the functions intended. Organizations may determine that, in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, the detection of malicious downloads, or the detection of maliciousness when attempting to open or execute files.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: NIST SP 800-83, 800-125B, 800-177; FBI CJIS CSP v5.9.	AC-4, AC-19, CM-3, CM-8, IR-4, MA-3, MA-4, PL-9, RA-5, SC-7, SC-23, SC-26, SC-28, SC-44, SI-2, SI-4, SI-7, SI-8, SI-15.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy; system and information integrity procedures; configuration management policy and procedures; procedures addressing malicious code protection; malicious code protection mechanisms; records of malicious code protection updates; system design documentation; system configuration settings and associated documentation; scan results from malicious code protection mechanisms; record of actions initiated by malicious code protection mechanisms in response to malicious code detection; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for malicious code protection; organizational personnel with configuration management responsibilities.

Test: Organizational processes for employing, updating, and configuring malicious code protection mechanisms; organizational processes for addressing false positives and resulting potential impacts; automated mechanisms supporting and/or implementing, employing, updating, and configuring malicious code protection mechanisms; automated mechanisms supporting and/or implementing malicious code scanning and subsequent actions.

SI-03(01): CENTRAL MANAGEMENT

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

This control is withdrawn and incorporated into PL-09 but still referenced in the FBI CJIS Security Policy v5.9. Please see PL-09.

SI-03(02): AUTOMATIC UPDATES

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

This control is withdrawn and incorporated into SI-03 but still referenced in the FBI CJIS Security Policy v5.9. Please see SI-03.

SI-04: INFORMATION SYSTEM MONITORING

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Monitor the system to detect:

   1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: objectives defined in the Information Security Program Plan or the System Security Plan (SSP); and
   2. Unauthorized local, network, and remote connections;

b. Identify unauthorized use of the system through the following techniques and methods: techniques and methods as defined in the SSP;

c. Invoke internal monitoring capabilities or deploy monitoring devices:

   1. Strategically within the system to collect organization-determined essential information; and
   2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;

d. Analyze detected events and anomalies;

e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;

f. Obtain legal opinion regarding system monitoring activities; and

g. Provide system monitoring information as defined in the applicable SSP to personnel or roles identified in the SSP as needed and at the frequency defined in the SSP.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — The DFPS Commissioner or his/her designated representative and DFPS Chief Information Security Officer shall establish a security strategy that includes perimeter protection. [Source: DIR Control Standards Catalog SI-4]

Std.02 — The Department of Information Resources will provide security information management services to include external network monitoring, scanning, and alerting for state organizations that utilize State information resources as specified in Chapters 2054 and 2059, Government Code. Perimeter security controls may include

some or all of the following components: DMZ, firewall, intrusion detection or prevention system, or router. [Source: DIR Control Standards Catalog SI-4]

Std.03 — Configure systems to address all applicable monitoring objectives in accordance with the Information Security Program Plan, including but not limited to:

a. Impact of security changes to the information system;
b. Unauthorized use of the system;
c. Information system attacks; and
d. Identified specific types of transactions of interest.

Std.04 — Intrusion Detection/Prevention System (IDS/IPS) devices must be installed at network perimeter points.

SUPPLEMENTAL GUIDANCE

System monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at external interfaces to the system. Internal monitoring includes the observation of events occurring within the system. Organizations monitor systems by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives guide and inform the determination of the events. System monitoring capabilities are achieved through a variety of tools and techniques, including intrusion detection and prevention systems, malicious code protection software, scanning tools, audit record monitoring software, and network monitoring software.

Depending on the security architecture, the distribution and configuration of monitoring devices may impact throughput at key internal and external boundaries as well as at other locations across a network due to the introduction of network throughput latency. If throughput management is needed, such devices are strategically located and deployed as part of an established organization-wide security architecture. Strategic locations for monitoring devices include selected perimeter locations and near key servers and server farms that support critical applications. Monitoring devices are typically employed at the managed interfaces associated with controls SC-07 and AC-17. The information collected is a function of the organizational monitoring objectives and the capability of systems to support such objectives. Specific types of transactions of interest include Hypertext Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. System monitoring is an integral part of organizational continuous monitoring and incident response programs, and output from system monitoring serves as input to those programs. System monitoring requirements, including the need for specific types of system monitoring, may be referenced in other controls (e.g., AC-02g, AC-17(01), CM-03f, CM-06d, MA-03a, MA-04a, SC-07a, SC-07(24)b, SC-18b). Adjustments to levels of system monitoring are based on law enforcement information, intelligence information, or other sources of information. The legality of system monitoring activities is based on applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; FIPS 140; NIST SP 800-61, 800-83, 800-92, 800-94, 800-137; FBI CJIS CSP v5.9.	AC-2, AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, AU-13, AU-14, CA-7, CM-3, CM-6, CM-8, CM-11, IA-10, IR-4, MA-3, MA-4, PL-9, PM-12, RA-5, RA-10, SC-5, SC-7, SC-18, SC-26, SC-31, SC-35, SC-36, SC-37, SC-43, SI-3, SI-6, SI-7, SR-9, SR-10.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy; system and information integrity procedures; procedures addressing system monitoring tools and techniques; continuous monitoring strategy; facility diagram/layout; system design documentation; system monitoring tools and techniques documentation; locations within the system where monitoring devices are deployed; system configuration settings and associated documentation; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring the system.

Test: Organizational processes for system monitoring; automated mechanisms supporting and/or implementing system monitoring capabilities.

SI-04(01): SYSTEM-WIDE INTRUSION DETECTION SYSTEM

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization connects and configures individual intrusion detection tools into an information system-wide intrusion detection system.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Ensure that intrusion detection information is aggregated to a centralized security information and event management (SIEM) or centralized audit repository for analysis and review by DFPS Office of Information Security:

a. Information is provided to DFPS Office of Information Security in a searchable format compliant with DFPS, state, and federal requirements;
b. Intrusion detection information sources include network and host-based IDS/IPS, systems, appliances, devices, services, and applications (including databases); and
c. DFPS Office of Information Security-directed audit information collection rules/requests (for example, sources, queries, data calls) are implemented/provided within the timeframe specified in the request.

Std.02 — Raw audit records and raw security information/results from relevant automated tools must be available in an unaltered format to DFPS Office of Information Security..

SUPPLEMENTAL GUIDANCE

Linking individual intrusion detection tools into a system-wide intrusion detection system provides additional coverage and effective detection capabilities. The information contained in one intrusion detection tool can be shared widely across the organization, making the system-wide detection capability more robust and powerful

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog.	None.

Federal: OMB A-130; FIPS 140; NIST SP 800-61, 800-83, 800-92, 800-94, 800-137; FBI CJIS CSP v5.9.	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy; system and information integrity procedures; procedures addressing system monitoring tools and techniques; continuous monitoring strategy; facility diagram/layout; system design documentation; system monitoring tools and techniques documentation; locations within the system where monitoring devices are deployed; system configuration settings and associated documentation; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring the system.

Test: Organizational processes for system monitoring; automated mechanisms supporting and/or implementing system monitoring capabilities.

SI-04(02): AUTOMATED TOOLS FOR REAL-TIME ANALYSIS

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization employs automated tools to support near real-time analysis of events.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Ensure that intrusion detection information is aggregated to a centralized security information and event management (SIEM) or centralized audit repository for analysis and review by DFPS Office of Information Security:

d. Information is provided to DFPS Office of Information Security in a searchable format compliant with DFPS, state, and federal requirements;
e. Audit record sources include network and host-based IDS/IPS, systems, appliances, devices, services, and applications (including databases); and
f. DFPS Office of Information Security-directed audit information collection rules/requests (for example, sources, queries, data calls) are implemented/provided within the timeframe specified in the request.

Std.02 — Raw audit records and raw security information/results from relevant automated tools must be available in an unaltered format to DFPS Office of Information Security..

SUPPLEMENTAL GUIDANCE

Automated tools and mechanisms include host-based, network-based, transport-based, or storage-based event monitoring tools and mechanisms or security information and event management (SIEM) technologies that provide real-time analysis of alerts and notifications generated by organizational systems. Automated monitoring techniques can create unintended privacy risks because automated controls may connect to external or

otherwise unrelated systems. The matching of records between these systems may create linkages with unintended consequences. Organizations assess and document these risks in their privacy impact assessment and make determinations that are in alignment with their privacy program plan.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; FIPS 140; NIST SP 800-61, 800-83, 800-92, 800-94, 800-137; FBI CJIS CSP v5.9.	PM-23, PM-25.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy; system and information integrity procedures; procedures addressing system monitoring tools and techniques; system design documentation; system monitoring tools and techniques documentation; system configuration settings and associated documentation; system audit records; system security plan; privacy plan; privacy program plan; privacy impact assessment; privacy risk management documentation; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security and privacy responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring the system; organizational personnel responsible for incident response/management.

Test: Organizational processes for the near real-time analysis of events; organizational processes for system monitoring; automated mechanisms supporting and/or implementing system monitoring; automated mechanisms/tools supporting and/or implementing an analysis of events

SI-04(04): INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization:

a. Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;

b. Monitor inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions as defined in system monitoring plans.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Aggregated inbound and outbound communications information must be searchable by DFPS Information Security:

a. Information is provided to DFPS Office of Information Security in a format compliant with DFPS, state, and federal (e.g., Continuous Diagnostics and Mitigation) requirements;

b. Information sources include traffic analysis of information from local analysis tools and directly from any information technology component in an environment requiring a DFPS Authority to Operate (ATO); and

c. DFPS Office of Information Security directed aggregated inbound and outbound communications traffic (for example, sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.

Std.02 — Raw event information must be available in an unaltered format to DFPS Office of Information Security.

Std.03 — Where a system cannot monitor inbound and outbound communications traffic, provide a monitoring capability on a separate system to monitor localized, targeted, and network-wide events.

SUPPLEMENTAL GUIDANCE

Unusual or unauthorized activities or conditions related to system inbound and outbound communications traffic includes internal traffic that indicates the presence of malicious code or unauthorized use of legitimate code or credentials within organizational systems or propagating among system components, signaling to external systems, and the unauthorized exporting of information. Evidence of malicious code or unauthorized use of legitimate code or credentials is used to identify potentially compromised systems or system components.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; FIPS 140; NIST SP 800-61, 800-83, 800-92, 800-94, 800-137; FBI CJIS CSP v5.9.	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy; system and information integrity procedures; procedures addressing system monitoring tools and techniques; system design documentation; system monitoring tools and techniques documentation; system configuration settings and associated documentation; system audit records; system security plan; privacy plan; privacy program plan; privacy impact assessment; privacy risk management documentation; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security and privacy responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring the system; organizational personnel responsible for incident response/management.

Test: Organizational processes for intrusion detection and system monitoring; automated mechanisms supporting and/or implementing intrusion detection and system monitoring capabilities; automated mechanisms supporting and/or implementing the monitoring of inbound and outbound communications traffic.

SI-04(05): SYSTEM-GENERATED ALERTS

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization alerts personnel or roles identified in the System Security Plan (SSP) when the following system-generated indications of compromise or potential compromise occur indicators defined in SI-04.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Alerts may be generated from a variety of sources, including audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers. Alerts can be automated and may be transmitted telephonically, by electronic mail messages, or by text messaging. Organizational personnel on the alert notification list can include system administrators, mission or business owners, system owners, information owners/stewards, senior agency information security officers, senior agency officials for privacy, system security officers, or privacy officers. In contrast to alerts generated by the system, alerts generated by organizations focus on information sources external to the system, such as suspicious activity reports and reports on potential insider threats.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; FIPS 140; NIST SP 800-61, 800-83, 800-92, 800-94, 800-137; FBI CJIS CSP v5.9.	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy; system and information integrity procedures; procedures addressing system monitoring tools and techniques; system design documentation; system monitoring tools and techniques documentation; system configuration settings and associated documentation; system audit records; system security plan; privacy plan; privacy program plan; privacy impact assessment; privacy risk management documentation; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security and privacy responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring the system; organizational personnel responsible for incident response/management.

Test: Organizational processes for intrusion detection and system monitoring; automated mechanisms supporting and/or implementing intrusion detection and system monitoring capabilities; automated mechanisms supporting and/or implementing the monitoring of inbound and outbound communications traffic.

SI-04(07): AUTOMATED RESPONSE TO SUSPICIOUS EVENTS

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization alerts personnel or roles identified in the System Security Plan (SSP) when the following system-generated indications of compromise or potential compromise occur indicators defined in SI-04.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Alerts may be generated from a variety of sources, including audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers. Alerts can be automated and may be transmitted telephonically, by electronic mail messages, or by text messaging. Organizational personnel on the alert notification list can include system administrators, mission or business owners, system owners, information owners/stewards, senior agency information security officers, senior agency officials for privacy, system security officers, or privacy officers. In contrast to alerts generated by the system, alerts generated by organizations focus on information sources external to the system, such as suspicious activity reports and reports on potential insider threats.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; FIPS 140; NIST SP 800-61, 800-83, 800-92, 800-94, 800-137; FBI CJIS CSP v5.9.	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy; system and information integrity procedures; procedures addressing system monitoring tools and techniques; system design documentation; system monitoring tools and techniques documentation; system configuration settings and associated documentation; alerts and notifications generated based on detected suspicious events; records of actions taken to terminate suspicious events; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; system developers; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring the system; organizational personnel responsible for the intrusion detection system.

Test: Organizational processes for intrusion detection and system monitoring; automated mechanisms supporting and/or implementing intrusion detection and system monitoring capabilities; automated mechanisms supporting and/or implementing notifications to incident response personnel; automated mechanisms supporting and/or implementing actions to terminate suspicious events.

SI-04(09): TESTING OF MONITORING TOOLS AND MECHANISMS

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization test intrusion-monitoring tools and mechanisms on an annual basis.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Testing intrusion-monitoring tools and mechanisms is necessary to ensure that the tools and mechanisms are operating correctly and continue to satisfy the monitoring objectives of organizations. The frequency and depth of testing depends on the types of tools and mechanisms used by organizations and the methods of deployment.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; FIPS 140; NIST SP 800-61, 800-83, 800-92, 800-94, 800-137; FBI CJIS CSP v5.9.	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy; system and information integrity procedures; procedures addressing the testing of system monitoring tools and techniques; documentation providing evidence of testing intrusion-monitoring tools; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring the system; organizational personnel responsible for the intrusion detection system.

Test: Organizational processes for intrusion detection and system monitoring; automated mechanisms supporting and/or implementing intrusion detection and system monitoring capabilities; automated mechanisms supporting and/or implementing the testing of intrusion-monitoring tools.

SI-04(11): ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization analyzes outbound communications traffic at the external boundary of the information system and interior points within the system (e.g., subnetworks, subsystems) that process CJI to discover anomalies.

AGENCY IMPLEMENTATION STANDARDS

Std.01 – Monitor inbound and outbound communications for unusual or unauthorized activities.

Std.02 – Send individual intrusion detection logs to a central logging facility where correlation and analysis will be accomplished as a system wide intrusion detection effort.

Std.03 – Employ automated tools to support near-real-time analysis of events in support of detecting system-level attacks.

SUPPLEMENTAL GUIDANCE

Organization-defined interior points include subnetworks and subsystems. Anomalies within organizational systems include large file transfers, long-time persistent connections, attempts to access information from unexpected locations, the use of unusual protocols and ports, the use of unmonitored network protocols (e.g., IPv6 usage during IPv4 transition), and attempted communications with suspected malicious external addresses.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; FIPS 140; NIST SP 800-61, 800-83, 800-92, 800-94, 800-137; FBI CJIS CSP v5.9.	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy; system and information integrity procedures; procedures addressing system monitoring tools and techniques; system design documentation; network diagram; system monitoring tools and techniques documentation; system configuration settings and associated documentation; system monitoring logs or records; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring the system; organizational personnel responsible for the intrusion detection system.

Test: Organizational processes for intrusion detection and system monitoring; automated mechanisms supporting and/or implementing intrusion detection and system monitoring capabilities; automated mechanisms supporting and/or implementing the analysis of communications traffic.

SI-04(12): AUTOMATED ALERTS

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: indicators defined in SI-04.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Organizational personnel on the system alert notification list include system administrators, mission or business owners, system owners, senior agency information security officer, senior agency official for privacy, system security officers, or privacy officers. Automated organization-generated alerts are the security alerts generated by organizations and transmitted using automated means. The sources for organization-generated alerts are focused on other entities such as suspicious activity reports and reports on potential insider threats. In contrast to alerts generated by the organization, alerts generated by the system in SI-4(5) focus on information sources that are internal to the systems, such as audit records.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; FIPS 140; NIST SP 800-61, 800-83, 800-92, 800-94, 800-137; FBI CJIS CSP v5.9.	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy; system and information integrity procedures; procedures addressing system monitoring tools and techniques; system design documentation; system monitoring tools and techniques documentation; system configuration settings and associated documentation; list of inappropriate or unusual activities with security and privacy implications that trigger alerts; suspicious activity reports; alerts provided to security and privacy personnel; system monitoring logs or records; system audit records; system security plan; privacy plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security and privacy responsibilities; system developers; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring the system; organizational personnel responsible for the intrusion detection system.

Test: Organizational processes for intrusion detection and system monitoring; automated mechanisms supporting and/or implementing intrusion detection and system monitoring capabilities; automated mechanisms supporting and/or implementing automated alerts to security personnel.

SI-04(14): WIRELESS INTRUSION DETECTION

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Wireless signals may radiate beyond organizational facilities. Organizations proactively search for unauthorized wireless connections, including the conduct of thorough scans for unauthorized wireless access points. Wireless scans are not limited to those areas within facilities containing systems but also include areas outside of facilities to verify that unauthorized wireless access points are not connected to organizational systems.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; FIPS 140; NIST SP 800-61, 800-83, 800-92, 800-94, 800-137; FBI CJIS CSP v5.9.	AC-18, IA-3.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy; system and information integrity procedures; procedures addressing system monitoring tools and techniques; system design documentation; system monitoring tools and techniques documentation; system configuration settings and associated documentation; system protocols; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring the system; organizational personnel responsible for the intrusion detection system.

Test: Organizational processes for intrusion detection; automated mechanisms supporting and/or implementing a wireless intrusion detection capability.

SI-04(15): WIRELESS TO WIRELINE COMMUNICATIONS

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization employs an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Wireless networks are inherently less secure than wired networks. For example, wireless networks are more susceptible to eavesdroppers or traffic analysis than wireline networks. When wireless to wireline communications exist, the wireless network could become a port of entry into the wired network. Given the greater facility of unauthorized network access via wireless access points compared to unauthorized wired network access from within the physical boundaries of the system, additional monitoring of transitioning traffic between wireless and wired networks may be necessary to detect malicious activities. Employing intrusion detection systems to monitor wireless communications traffic helps to ensure that the traffic does not contain malicious code prior to transitioning to the wireline network.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; FIPS 140; NIST SP 800-61, 800-83, 800-92, 800-94, 800-137; FBI CJIS CSP v5.9.	AC-18.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy; system and information integrity procedures; procedures addressing system monitoring tools and techniques; system design documentation; system monitoring tools and techniques documentation; system configuration settings and associated documentation; system protocols documentation; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring the system; organizational personnel responsible for the intrusion detection system.

Test: Organizational processes for intrusion detection and system monitoring; automated mechanisms supporting and/or implementing intrusion detection and system monitoring capabilities; automated mechanisms supporting and/or implementing a wireless intrusion detection capability

SI-04(23): HOST-BASED DEVICES

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization implements host-based monitoring mechanisms on all systems, appliances, devices, services, and applications.

AGENCY IMPLEMENTATION STANDARDS

Std.01 - Devices and appliances that do not support a host-based intrusion detection system/intrusion prevention system (IDS/IPS) sensor capability must be documented in the applicable Information System Risk Assessment and System Security Plan.

SUPPLEMENTAL GUIDANCE

Host-based monitoring collects information about the host (or system in which it resides). System components in which host-based monitoring can be implemented include servers, notebook computers, and mobile devices. Organizations may consider employing host-based monitoring mechanisms from multiple product developers or vendors.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; FIPS 140; NIST SP 800-61, 800-83, 800-92, 800-94, 800-137; FBI CJIS CSP v5.9.	AC-18, AC-19.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy; system and information integrity procedures; procedures addressing system monitoring tools and techniques; system design documentation; host-based monitoring mechanisms; system monitoring tools and techniques documentation; system configuration settings and associated documentation; list of system components requiring host-based monitoring; system monitoring logs or records; system audit records; system security plan; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring system hosts.

Test: Organizational processes for system monitoring; automated mechanisms supporting and/or implementing host-based monitoring capability.

SI-05: SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Receive system security alerts, advisories, and directives from external organizations per Std.02 on an ongoing basis;

b. Generate internal security alerts, advisories, and directives as deemed necessary;

c. Disseminate security alerts, advisories, and directives to personnel or roles defined in Std.03; and

d. Implement security directives in accordance with established time frames or notify the issuing organization of the degree of noncompliance.

AGENCY IMPLEMENTATION STANDARDS

Std.01 – DFPS must receive information system security alerts/advisories on a regular basis, issues alerts/advisories to appropriate personnel, and takes appropriate actions in response. [Source: DIR Control Standards Catalog SI-5]

Std.02 — External organizations from which system security alerts, advisories, and directives must be received include:

a. Cybersecurity and Infrastructure Security Agency (CISA);

b. Texas Department of Information Resources (DIR); and

c. Contracted service providers.

Std.03 — Security alerts, advisories, and directives must be disseminated to personnel or roles with information security, system administration, monitoring, or incident handling responsibilities, as identified in access control policies.

SUPPLEMENTAL GUIDANCE

The Cybersecurity and Infrastructure Security Agency (CISA) generates security alerts and advisories to maintain situational awareness throughout the Federal Government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance with security directives is essential due to the critical nature of many of these directives and the potential (immediate) adverse effects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner. External organizations include supply chain partners, external mission or business partners, external service providers, and other peer or supporting organizations.

Alerts and advisories may be received and disseminated from other entities, including but not limited to agency partners, peers, vendors not yet contracted, and national cybersecurity organizations such as SANS.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: NIST SP 800-40; FBI CJIS CSP v5.9.	PM-15, RA-5, SI-2.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy; system and information integrity procedures; procedures addressing security alerts, advisories, and directives; records of security alerts and advisories; system security plan; other relevant documents or records.

Interview: Organizational personnel with security alert and advisory responsibilities; organizational personnel implementing, operating, maintaining, and using the system; organizational personnel, organizational elements, and/or external organizations to whom alerts, advisories, and directives are to be disseminated; system/network administrators; organizational personnel with information security responsibilities.

Test: Organizational processes for defining, receiving, generating, disseminating, and complying with security alerts, advisories, and directives; automated mechanisms supporting and/or implementing the definition, receipt, generation, and dissemination of security alerts, advisories, and directives; automated mechanisms supporting and/or implementing security directives.

SI-05(01): AUTOMATED ALERTS AND ADVISORIES

Priority: P1

Baseline(s): High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization broadcasts security alert and advisory information throughout the organization using automated mechanisms as identified in applicable System Security Plans (SSPs).

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

The significant number of changes to organizational systems and environments of operation requires the dissemination of security-related information to a variety of organizational entities that have a direct interest in the success of organizational mission and business functions. Based on information provided by security alerts and advisories, changes may be required at one or more of the three levels related to the management of risk, including the governance level, mission and business process level, and the information system level.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: NIST SP 800-40; FBI CJIS CSP v5.9.	None.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy; system and information integrity procedures; procedures addressing security alerts, advisories, and directives; system design documentation; system configuration settings and associated documentation; automated mechanisms supporting the distribution of security alert and advisory information; records of security alerts and advisories; system audit records; system security plan; other relevant documents or records.

Interview: Organizational personnel with security alert and advisory responsibilities; organizational personnel implementing, operating, maintaining, and using the system; organizational personnel, organizational elements, and/or external organizations to whom alerts and advisories are to be disseminated; system/network administrators; organizational personnel with information security responsibilities.

Test: Organizational processes for defining, receiving, generating, and disseminating security alerts and advisories; automated mechanisms supporting and/or implementing the dissemination of security alerts and advisories.

SI-06: SECURITY AND PRIVACY FUNCTION VERIFICATION

Priority: P1

Baseline(s): High	Overlay(s): DIR

CONTROL REQUIREMENTS

The organization:

a. Verify the correct operation of security and privacy functions defined in the System Security Plan (SSP);

b. Perform the verification of the functions specified in SI-06a at system startup and restart, upon command by a user with appropriate privilege, and periodically every 30 days;

c. Alert personnel or roles as identified in the SSP to failed security and privacy verification tests; and

d. Shut the system down, restart the system, or take other defined alternative action(s) as specified in the SSP when anomalies are discovered.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Transitional states for systems include system startup, restart, shutdown, and abort. System notifications include hardware indicator lights, electronic alerts to system administrators, and messages to local computer consoles. In contrast to security function verification, privacy function verification ensures that privacy functions operate as expected and are approved by the senior agency official for privacy or that privacy attributes are applied or used as expected.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130;	CA-7, CM-4, CM-6, SI-7.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy; system and information integrity procedures; procedures addressing security and privacy function verification; system design documentation; system configuration settings and associated documentation; alerts/notifications of failed security verification tests; list of system transition states requiring security functionality verification; system audit records; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with security alert and advisory responsibilities; organizational personnel implementing, operating, maintaining, and using the system; organizational personnel, organizational elements, and/or external organizations to whom alerts and advisories are to be disseminated; system/network administrators; organizational personnel with information security responsibilities.

Test: Organizational processes for defining, receiving, generating, and disseminating security alerts and advisories; automated mechanisms supporting and/or implementing the dissemination of security alerts and advisories.

SI-07: SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The organization:

a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: organization-controlled software, firmware, and information as identified in the System Security Plan (SSP); and

b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: actions as identified in the SSP.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Tools and mechanisms must be, as feasible:

a. Enabled on each device or system on the network, so long as performance is not impaired;

b. Checked against baselines to effectively verify variations from normal work-related activities; and

c. Able to provide a means to determine the date and time a resource was last accessed or modified.

SUPPLEMENTAL GUIDANCE

Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity. Software includes operating systems (with key internal components, such as kernels or drivers), middleware, and applications. Firmware interfaces include Unified Extensible Firmware Interface (UEFI) and Basic Input/Output System (BIOS). Information includes personally identifiable information and metadata that contains security and privacy attributes associated with information. Integrity-checking mechanisms—including parity checks, cyclical redundancy checks, cryptographic hashes, and associated tools—can automatically monitor the integrity of systems and hosted applications.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** Texas Cybersecurity Framework; DIR Security Control Standards Catalog. **Federal**: OMB A-130; FIPS 140, 180, 186, 202; NIST SP 800-70, 800-147; FBI CJIS CSP v5.9.	AC-4, CM-3, CM-7, CM-8, MA-3, MA-4, RA-5, SA-8, SA-9, SA-10, SC-8, SC-12, SC-13, SC-28, SC-37, SI-3, SR-3, SR-4, SR-5, SR-6, SR-9, SR-10, SR-11.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy; system and information integrity procedures; procedures addressing software, firmware, and information integrity; personally identifiable information processing policy; system design documentation; system configuration settings and associated documentation; integrity verification tools and associated documentation; records generated or triggered by integrity verification tools regarding unauthorized software, firmware, and information changes; system audit records; system security plan; privacy plan; other relevant documents or records

Interview: Organizational personnel responsible for software, firmware, and/or information integrity; organizational personnel with information security and privacy responsibilities; system/network administrators.

Test: Software, firmware, and information integrity verification tools.

SI-07(01): INTEGRITY CHECKS

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization performs an integrity check of software, firmware, and information at system startup and at least once per day.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Security-relevant events include, for example, the identification of a new threat to which organizational information systems are susceptible, and the installation of new hardware, software, or firmware. Transitional states include, for example, system startup, restart, shutdown, and abort.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; FIPS 140, 180, 186, 202; NIST SP 800-70, 800-147; FBI CJIS CSP v5.9.	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy; system and information integrity procedures; procedures addressing software, firmware, and information integrity testing; system design documentation; system configuration settings and associated documentation; integrity verification tools and associated documentation; records of integrity scans; system security plan; other relevant documents or records.

Interview: Organizational personnel responsible for software, firmware, and/or information integrity; organizational personnel with information security responsibilities; system/network administrators; system developer.

Test: Software, firmware, and information integrity verification tools.

SI-07(06): CRYPTOGRAPHIC PROTECTION

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The information system implements cryptographic mechanisms to detect unauthorized changes to software, firmware, and information.

AGENCY IMPLEMENTATION STANDARDS

Std.01 – The information system implements cryptographic mechanisms in accordance with SC-13/

SUPPLEMENTAL GUIDANCE

Cryptographic mechanisms used for the protection of integrity include, for example, digital signatures and the computation and application of signed hashes using asymmetric cryptography, protecting the confidentiality of the key used to generate the hash, and using the public key to verify the hash information.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; FIPS 140, 180, 186, 202; NIST SP 800-70, 800-147; FBI CJIS CSP v5.9.	SC-12, SC-13.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy; system and information integrity procedures; procedures addressing software, firmware, and information integrity; system design documentation; system configuration settings and associated documentation; cryptographic mechanisms and associated documentation; records of detected unauthorized changes to software, firmware, and information; system audit records; system security plan; other relevant documents or records.

Interview: Organizational personnel responsible for software, firmware, and/or information integrity; organizational personnel with information security responsibilities; system/network administrators; system developer.

Test: Software, firmware, and information integrity verification tools; cryptographic mechanisms implementing software, firmware, and information integrity.

SI-07(07): INTEGRATION OF DETECTION AND RESPONSE

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization incorporates the detection of unauthorized changes into the organizational incident response capability: security-relevant changes to the system as defined in the System Security Plan (SSP).

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Where the system cannot detect unauthorized security-relevant changes, compensating controls (for example, manual procedures) must be employed. [Source: NIST SP 800-82]

SUPPLEMENTAL GUIDANCE

Integrating detection and response helps to ensure that detected events are tracked, monitored, corrected, and available for historical purposes. Maintaining historical records is important for being able to identify and discern adversary actions over an extended time period and for possible legal actions. Security-relevant changes include unauthorized changes to established configuration settings or the unauthorized elevation of system privileges.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; FIPS 140, 180, 186, 202; NIST SP 800-70, 800-147; FBI CJIS CSP v5.9.	AU-2, AU-6, IR-4, IR-5, SI-4.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy; system and information integrity procedures; procedures addressing software, firmware, and information integrity; procedures addressing incident response; system design documentation; system configuration settings and associated documentation; incident response records; audit records; system security plan; other relevant documents or records.

Interview: Organizational personnel responsible for software, firmware, and/or information integrity; organizational personnel with information security responsibilities; organizational personnel with incident response responsibilities.

Test: Organizational processes for incorporating the detection of unauthorized security-relevant changes into the incident response capability; software, firmware, and information integrity verification tools; automated mechanisms supporting and/or implementing the incorporation of detection of unauthorized security-relevant changes into the incident response capability.

SI-08: SPAM PROTECTION

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization:

a. Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages; and

b. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

System entry and exit points include firewalls, remote-access servers, electronic mail servers, web servers, proxy servers, workstations, notebook computers, and mobile devices. Spam can be transported by different means, including email, email attachments, and web accesses. Spam protection mechanisms include signature definitions.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: NIST SP 800-45, 800-177; FBI CJIS CSP v5.9.	PL-9, SC-5, SC-7, SC-38, SI-3, SI-4.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy; system and information integrity procedures; configuration management policies and procedures (CM-01); procedures addressing spam protection; spam protection mechanisms; records of spam protection updates; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

Interview: Organizational personnel responsible for spam protection; organizational personnel with information security responsibilities; system/network administrators; system developer.

Test: Organizational processes for implementing spam protection; automated mechanisms supporting and/or implementing spam protection.

SI-08(01): CENTRAL MANAGEMENT

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

This control is withdrawn and incorporated into PL-09 but still referenced in the FBI CJIS Security Policy v5.9. Please see PL-09.

SI-08(02): AUTOMATIC UPDATES

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CJIS

CONTROL REQUIREMENTS

The information system automatically updates spam protection mechanisms.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Using automated mechanisms to update spam protection mechanisms helps to ensure that updates occur on a regular basis and provide the latest content and protection capabilities

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: NIST SP 800-45, 800-177; FBI CJIS CSP v5.9.	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy; system and information integrity procedures; procedures addressing spam protection; spam protection mechanisms; records of spam protection updates; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

Interview: Organizational personnel responsible for spam protection; organizational personnel with information security responsibilities; system/network administrators; system developer.

Test: Organizational processes for spam protection; automated mechanisms supporting and/or implementing automatic updates to spam protection mechanisms.

SI-10: INFORMATION INPUT VALIDATION

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The information system checks the validity of the following information inputs: all inputs to web/application servers, database servers, and any system or application input (as defined in applicable System Security Plans (SSPs)).

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Configure systems to:

a. Check all arguments or input data strings submitted by users, external processes, or untrusted internal processes as close to the point of origin as possible, and before passing to any other application or interpreter;

b. Validate all values that originate externally to the application program itself, including arguments, environment variables, and information system parameters;

c. Reject and discard invalid values, parameters, strings, or objects.

Std.02 — For Web and mobile apps, test user input form fields for malicious commands (e.g. SQL injection).

SUPPLEMENTAL GUIDANCE

Checking the valid syntax and semantics of system inputs—including character set, length, numerical range, and acceptable values—verifies that inputs match specified definitions for format and content. For example, if the organization specifies that numerical values between 1-100 are the only acceptable inputs for a field in a given application, inputs of "387," "abc" or "%K%" are invalid inputs and are not accepted as input to the system. Valid inputs are likely to vary from field to field within a software application. Applications typically follow well-defined protocols that use structured messages (i.e., commands or queries) to communicate between software modules or system components. Structured messages can contain raw or unstructured data interspersed with metadata or control information. If software applications use attacker-supplied inputs to construct structured messages without properly encoding such messages, then the attacker could insert malicious commands or special characters that can cause the data to be interpreted as control information or metadata. Consequently, the module or component that receives the corrupted output will perform the wrong operations or otherwise interpret the data incorrectly. Prescreening inputs prior to passing them to interpreters prevents the content

from being unintentionally interpreted as commands. Input validation ensures accurate and correct inputs and prevents attacks such as cross-site scripting and a variety of injection attacks.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: OMB A-130; FBI CJIS CSP v5.9.	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy; system and information integrity procedures; access control policy and procedures; separation of duties policy and procedures; procedures addressing information input validation; documentation for automated tools and applications to verify the validity of information; list of information inputs requiring validity checks; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records.

Interview: Organizational personnel responsible for information input validation; organizational personnel with information security responsibilities; system/network administrators; system developer.

Test: Automated mechanisms supporting and/or implementing validity checks on information inputs.

SI-11: ERROR HANDLING

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CJIS

CONTROL REQUIREMENTS

The information system:

a. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; and

b. Reveal error messages only to authorized personnel as identified in the System Security Plan (SSP).

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Perform risk analysis to identify error conditions to be identified and required timelines for error handling.

Std.02 — Error messages revealed to users must not include file pathnames or system architecture information nor should error messages reveal details about the internal functionality of the application.

Std.03 — Error messages and alerts revealed to the administrator should include file pathnames or system architecture information, may include criticality or severity level if determined, and must be written to the application's error log and audit trail.

Std.04 — Turn off debugging on production web servers.

SUPPLEMENTAL GUIDANCE

Organizations consider the structure and content of error messages. The extent to which systems can handle error conditions is guided and informed by organizational policy and operational requirements. Exploitable information includes stack traces and implementation details; erroneous logon attempts with passwords mistakenly entered as the username; mission or business information that can be derived from, if not stated explicitly by, the information recorded; and personally identifiable information, such as account numbers, social security numbers, and credit card numbers. Error messages may also provide a covert channel for transmitting information.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: FBI CJIS CSP v5.9.	AU-2, AU-3, SC-31, SI-2, SI-15.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy; system and information integrity procedures; procedures addressing system error handling; system design documentation; system configuration settings and associated documentation; documentation providing the structure and content of error messages; system audit records; system security plan; other relevant documents or records.

Interview: Organizational personnel responsible for information input validation; organizational personnel with information security responsibilities; system/network administrators; system developer.

Test: Organizational processes for error handling; automated mechanisms supporting and/or implementing error handling; automated mechanisms supporting and/or implementing the management of error messages.

SI-12: INFORMATION HANDLING AND RETENTION

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): DIR, CJIS. Privacy

CONTROL REQUIREMENTS

The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Handle and retain output from the information system, whether hardcopy or digital, in accordance with applicable laws, standards, and operational requirements. [Source: DIR Control Standards Catalog SI-12]

Std.02 — Document output handling, media protection. and retention requirements in the System Security Plan (SSP) and retain and dispose of information system output accordingly.

SUPPLEMENTAL GUIDANCE

Information management and retention requirements cover the full life cycle of information, in some cases extending beyond system disposal. Information to be retained may also include policies, procedures, plans, reports, data output from control implementation, and other types of administrative information. The National Archives and Records Administration (NARA) provides federal policy and guidance on records retention and schedules. If organizations have a records management office, consider coordinating with records management personnel. Records produced from the output of implemented controls that may require management and retention include, but are not limited to: AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PM-1, PS-1, PT-1, RA-1, SA-1, SC-1, SI-1, SR-1, AC-6(9), AT-4, AU-12, CA-2, CA-3, CA-5, CA-6, CA-7, CA-8, CA-9, CM-2, CM-3, CM-4, CM-6, CM-8, CM-9, CM-12, CM-13, CP-2, IR-6, IR-8, MA-2, MA-4, PE-2, PE-8, PE-16, PE-17, PL-2, PL-4, PL-7, PL-8, PM-5, PM-8, PM-9, PM-18, PM-21, PM-27, PM-28, PM-30, PM-31, PS-2, PS-6, PS-7, PT-2, PT-3, PT-7, RA-2, RA-3, RA-5, RA-8, SA-4, SA-5, SA-8, SA-10, SI-4, SR-2, SR-4, SR-8.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: USC 2901; OMB A-130; FBI CJIS CSP v5.9.	AC-16, AU-5, AU-11, CA-2, CA-3, CA-5, CA-6, CA-7, CA-9, CM-5, CM-9, CP-2, IR-8, MP-2, MP-3, MP-4, MP-6, PL-2, PL-4, PM-4, PM-8, PM-9, PS-2, PS-6, PT-2, PT-3, RA-2, RA-3, SA-5, SA-8, SR-2.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy; system and information integrity procedures; personally identifiable information processing policy; records retention and disposition policy; records retention and disposition procedures; federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements applicable to information management and retention; media protection policy; media protection procedures; audit findings; system security plan; privacy plan; privacy program plan; personally identifiable information inventory; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records.

Interview: Organizational personnel with information and records management, retention, and disposition responsibilities; organizational personnel with information security and privacy responsibilities; network administrators.

Test: Organizational processes for information management, retention, and disposition; automated mechanisms supporting and/or implementing information management, retention, and disposition.

SI-12(01): LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): Privacy

CONTROL REQUIREMENTS

The organization limits personally identifiable information being processed in the information life cycle to the following elements of personally identifiable information: elements of sensitive personal information (SPI) defined in accordance with the DFPS Data Classification Policy and identified in the privacy risk assessment.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Limiting the use of personally identifiable information throughout the information life cycle when the information is not needed for operational purposes helps to reduce the level of privacy risk created by a system. The information life cycle includes information creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposition. Risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to determining which elements of personally identifiable information may create risk.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; Data Classification Policy. **State:** Bus. & Comm. 521; DIR Security Control Standards Catalog. **Federal**: USC 2901; OMB A-130; FBI CJIS CSP v5.9.	PM-25.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy; system and information integrity procedures; personally identifiable information processing policy; personally identifiable information processing procedures; records retention and disposition policy; records retention and disposition procedures; federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements applicable to limiting personally identifiable information elements; personally identifiable information inventory; system audit records; audit findings; system security plan; privacy plan; privacy program plan; privacy impact assessment; privacy risk assessment documentation; data mapping documentation; other relevant documents or records.

Interview: Organizational personnel with information and records management, retention, and disposition responsibilities; organizational personnel with security and privacy responsibilities; network administrators.

Test: Organizational processes for information management and retention (including limiting personally identifiable information processing); automated mechanisms supporting and/or implementing limits to personally identifiable information processing.

SI-12(02) MINIMIZE PERSONALLY IDENTIFIABLE INFORMATION IN TESTING, TRAINING, AND RESEARCH

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): Privacy

CONTROL REQUIREMENTS

Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: techniques as defined in SI-19.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Where feasible, use fictional or synthetic information for research, testing, or training.

Std.02 — Where live data must be used for research or testing, purge data or sanitize systems at the conclusion of such activities.

Std.03 — Information acquired by DFPS or a component of the agency under a pledge of confidentiality and for exclusively statistical purposes shall be used by officers, employees, or agents of the agency exclusively for statistical purposes. [Source: OMB A-130 Appendix II Sec. 6]

SUPPLEMENTAL GUIDANCE

DFPS and agency components should protect the integrity and confidentiality of this information against unauthorized access, use, disclosure, modification, or destruction throughout the life cycle of the information. DFPS and agency components shall also adhere to legal requirements and should follow best practices for protecting the confidentiality of data, including training their employees and agents, and ensuring the physical and information system security of confidential information. [Source: OMB A-130 Appendix II Sec. 6]

Organizations can minimize the risk to an individual's privacy by employing techniques such as de-identification or synthetic data. Limiting the use of personally identifiable information throughout the information life cycle when the information is not needed for research, testing, or training helps reduce the level of privacy risk created by a system. Risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to determining the techniques to use and when to use them.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy; Data Classification Policy. **State:** Bus. & Comm. 521; DIR Security Control Standards Catalog. **Federal**: USC 2901; OMB A-130; FBI CJIS CSP v5.9.	PM-22, PM-25, SI-19.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy; system and information integrity procedures; personally identifiable information processing policy; personally identifiable information processing procedures; federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements applicable to minimizing the use of personally identifiable information in testing, training, and research; policy for the minimization of personally identifiable information used in testing, training, and research; procedures for the minimization of personally identifiable information used in testing, training, and research; documentation supporting minimization policy implementation (e.g., templates for testing, training, and research); data sets used for testing, training, and research; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records/

Interview: Organizational personnel with information and records management, retention, and disposition responsibilities; organizational personnel with information security and privacy responsibilities; network administrators; system developers; personnel with IRB responsibilities.

Test: Organizational processes for the minimization of personally identifiable information used in testing, training, and research; automated mechanisms supporting and/or implementing the minimization of personally identifiable information used in testing, training, and research/

SI-12(03): INFORMATION DISPOSAL

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): Privacy

CONTROL REQUIREMENTS

Use the following techniques to dispose of, destroy, or erase information following the retention period: techniques as outlined in MP-06.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Organizations can minimize both security and privacy risks by disposing of information when it is no longer needed. The disposal or destruction of information applies to originals as well as copies and archived records, including system logs that may contain personally identifiable information.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: USC 2901; OMB A-130; FBI CJIS CSP v5.9.	N/A

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy; system and information integrity procedures; personally identifiable information processing policy; personally identifiable information processing procedures; records retention and disposition policy; records retention and disposition procedures; laws, Executive Orders, directives, policies, regulations, standards, and operational requirements applicable to information disposal; media protection policy; media protection procedures; system audit records; audit findings; information disposal records; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records.

Interview: Organizational personnel with information and records management, retention, and disposition responsibilities; organizational personnel with information security and privacy responsibilities; network administrators.

Test: Organizational processes for information disposition; automated mechanisms supporting and/or implementing information disposition.

SI-16: MEMORY PROTECTION

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR

CONTROL REQUIREMENTS

Implement the following controls to protect the system memory from unauthorized code execution: detection, prevention, and recovery controls as specified in the System Security Plan (SSP).

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Controls employed to protect memory include data execution prevention and address space layout randomization. Data execution prevention controls can either be hardware-enforced or software-enforced with hardware enforcement providing the greater strength of mechanism.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** DIR Security Control Standards Catalog. **Federal**: USC 2901; OMB A-130; FBI CJIS CSP v5.9.	AC-25, SC-3, SI-7.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy; system and information integrity procedures; procedures addressing memory protection for the system; system design documentation; system configuration settings and associated documentation; list of security safeguards protecting system memory from unauthorized code execution; system audit records; system security plan; other relevant documents or records.

Interview: Organizational personnel responsible for memory protection; organizational personnel with information security responsibilities; system/network administrators; system developer.

Test: Automated mechanisms supporting and/or implementing safeguards to protect the system memory from unauthorized code execution.

SI-19: DE-IDENTIFICATION

Priority: P1

Baseline(s): N/A	Overlay(s): Privacy

CONTROL REQUIREMENTS

The organization:

a. Remove the following elements of personally identifiable information from datasets: all elements of personally identifiable information (PII) as defined in Std.02; and

b. Evaluate at least annually for effectiveness of de-identification.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — DFPS shall destroy or arrange for the destruction of customer records containing sensitive personal information within the business's custody or control that are not to be retained by the business by modifying the sensitive personal information in the records to make the information unreadable or indecipherable through any means. [Source: Bus. & Comm. 521.052(b)(3)]

Std.02 — Sensitive personal information (SPI) meeting the definitions in Texas Business and Commerce Code 521 must be de-identified when identifiers are no longer needed for the purpose for which the data was collected.

Std.03 — Where feasible and within the limits of technology, locate and remove or redact SPI and/or use anonymization and de-identification techniques to permit use of the retained information while reducing its sensitivity and reducing the risk resulting from disclosure.

SUPPLEMENTAL GUIDANCE

De-identification is the general term for the process of removing the association between a set of identifying data and the data subject. Many datasets contain information about individuals that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records. Datasets may also contain other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. Personally identifiable information is removed from datasets by trained individuals when such information is not (or no longer) necessary to satisfy the requirements envisioned for the data. For example, if the dataset is only used to produce aggregate statistics, the identifiers that are not needed for producing those statistics are removed. Removing identifiers improves privacy protection since information that is removed cannot be inadvertently disclosed or improperly used. Organizations may be subject to specific de-identification definitions or methods under applicable laws, regulations, or policies. Re-identification is a residual risk with de-identified data. Re-identification attacks can vary, including combining new datasets or other improvements in data analytics.

Maintaining awareness of potential attacks and evaluating for the effectiveness of the de-identification over time support the management of this residual risk.

Personally identifiable information (PII) is defined as:

Information that alone or in conjunction with other information identifies an individual, including an individual's name, Social Security number, date of birth, government-issued identification number, mother's maiden name, unique biometric data, such as the individual's fingerprint, voice print, and retina or iris image. The definition also includes unique electronic identification number, address, or routing code. [Source: Bus. & Comm. 521.002(a)(1)]

Sensitive personal information (SPI) is defined as:

An individual's first name or first initial and last name in combination with any one or more of the following unencrypted items: social security number, driver's license number or government-issued identification number, account number, credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account. Also, information that identifies an individual and relates to the physical or mental health or condition of the individual, the provision of health care to the individual, payment for the provision of health care to the individual. However, the term "sensitive personal information" does not include publicly available information that is lawfully made available to the public from the federal government or a state or local government. [Source: Bus.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** State References Bus. & Comm. 521 **Federal**: OMB A-130; NIST SP 800-188.	MP-6, PM-22, PM-23, PM-24, RA-2, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy; system and information integrity procedures; personally identifiable information processing policy; de-identification procedures; system configuration; datasets with personally identifiable information removed; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records.

Interview: Organizational personnel responsible for identifying unnecessary identifiers; organizational personnel responsible for removing personally identifiable information from datasets; organizational personnel with information security and privacy responsibilities.

Test: Automated mechanisms supporting and/or implementing the removal of personally identifiable information elements.

(SR) SUPPLY RISK CHAIN MANAGEMENT

DFPS Supply chain risk management (SCRM) is a systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities, and threats throughout the supply chain and developing mitigation strategies to combat those threats whether presented by the supplier, the supplies product and its subcomponents, or the supply chain (e.g., initial production, packaging, handling, storage, transport, mission operation, and disposal).

The intended audience for this Control includes, but is not limited to, information resource owners and custodians. The information resource owner, or their designee, is responsible for ensuring that supply risk chain measures described in this Control family are implemented by personnel with supply chain responsibilities (e.g. system/network administrators, information security analyst, etc.).

SUPPLY RISK CHAIN MANAGEMENT POLICY AND PROCEDURES	
Priority: P1	
Baseline(s): Low, Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization:

a. Develop, document, and disseminate to appropriate personnel:
   1. Organization-level supply chain risk management policy that:
      a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls;

b. Designate a senior management official as defined in the supply chain risk management policy to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; and

c. Review and update the current supply chain risk management:
   1. Policy every two (2) years and following major changes to legislation or security requirements; and
   2. Procedures every two (2) years and following major changes to legislation or security requirements.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Security requirements shall be identified, documented, and addressed in all phases of supply chain risk management.

Std.02 — The DFPS Chief Information Security Officer shall be responsible for:

a. Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks;

b. Providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities under 1 TAC 202; and

c. Developing and recommending policies and establishing procedures and practices, in cooperation with the agency Information Resources Manager, information-owners and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, or disclosure. [Source: 1 TAC 202.21(b)(3, 5, 8)]

SUPPLEMENTAL GUIDANCE

Supply chain risk management policy and procedures address the controls in the SR family as well as supply chain-related controls in other families that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures

contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of supply chain risk management policy and procedures.

Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations.

Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to supply chain risk management policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** 1 TAC 202.21(b)(3, 5, 8) **Federal**: Secure Technology Act; 41 CFR 201; EO 13873; NIST SP 800-12, 800-30, 800-39, 800-100, 800-161; CNSSD 505.	PM-9, PM-30, PS-8, SI-12.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Supply chain risk management policy; supply chain risk management procedures; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with supply chain risk management responsibilities; organizational personnel with information security and privacy responsibilities; organizational personnel with acquisition responsibilities; organizational personnel with enterprise risk management responsibilities.

SR-02: SUPPLY CHAIN RISK MANAGEMENT PLAN

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization:

a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services: all systems, system components, or system services under configuration management;

b. Review and update the supply chain risk management plan annually or as required, to address threat, organizational or environmental changes; and

c. Protect the supply chain risk management plan from unauthorized disclosure and modification.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Develop a supply chain risk management plan template in accordance with the guidance presented in NIST SP 800-161 (as amended).

Std.02 — Include external provider plan requirements in contracts as applicable.

Std.03 — Ensure that systems owners are aware of supply chain risk management (SCRM) plans.

Std.04 — Correlate identified critical components/services to the information about the supply chain, the supply chain infrastructure, historical data, and SDLC to identify critical supply chain paths. [Source: SP 800-161]

Std.05 — Protect against supply chain threats to the information system, system component, or information system service by employing best practices and methodologies; and wherever possible, selecting components that have been previously reviewed by other government entities (e.g., National Information Assurance Partnership (NIAP)) as part of a comprehensive, defense-in-breadth information security strategy. [Source: SP 800-53r4 SA- 12]

SUPPLEMENTAL GUIDANCE

The dependence on products, systems, and services from external providers, as well as the nature of the relationships with those providers, present an increasing level of risk to and organization. Threat actions that may increase security or privacy risks include unauthorized production, the insertion or use of counterfeits, tampering, theft, insertion of malicious software and hardware, and poor manufacturing and development practices in the supply chain. Supply chain risks can be endemic or systemic within a system element or component, a system, an organization, a sector, or the Nation. Managing supply chain risk is a complex, multifaceted undertaking that requires a coordinated effort across an organization to build trust relationships and communicate with internal and external stakeholders. Supply chain risk management (SCRM) activities include identifying and assessing risks, determining appropriate risk response actions, developing SCRM plans to document response actions, and monitoring performance against plans. The SCRM plan (at the system-level) is implementation specific, providing policy implementation, requirements, constraints, and implications. It can either be stand-alone or incorporated into system security and privacy plans. The SCRM plan addresses managing, implementation, and monitoring of SCRM controls and the development/sustainment of systems across the SDLC to support mission and business functions.

Because supply chains can differ significantly across and within organizations, SCRM plans are tailored to the individual program, organizational, and operational contexts. Tailored SCRM plans provide the basis for determining whether a technology, service, system component, or system is fit for purpose, and as such, the controls need to be tailored accordingly. Tailored SCRM plans help organizations focus their resources on the most critical mission and business functions based on mission and business requirements and their risk environment. Supply chain risk management plans include an expression of the supply chain risk tolerance for the organization, acceptable supply chain risk mitigation strategies or controls, a process for consistently evaluating and monitoring supply chain risk, approaches for implementing and communicating the plan, a description of and justification for supply chain risk mitigation measures taken, and associated roles and responsibilities.

Finally, supply chain risk management plans address requirements for developing trustworthy, secure, privacy-protective, and resilient system components and systems, including the application of the security design principles implemented as part of life cycle- based systems security engineering processes (see SA-08).

REFERENCES	**RELATED CONTROLS**

Agency: DFPS Information Security Policy. **State:** None. **Federal**: Secure Technology Act; 41 CFR 201; EO 13873; NIST SP 800-30, 800-39, 800-160-1, 800-161, 800-181; NIST IR 7622, 8272; CNSSD 505.	CA-2, CP-4, IR-4, MA-2, MA-6, PE-16, PL-2, PM-9, PM-30, RA-3, RA-7, SA-8, SI-4.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Supply chain risk management policy; supply chain risk management procedures; supply chain risk management plan; system and services acquisition policy; system and services acquisition procedures; procedures addressing supply chain protection; procedures for protecting the supply chain risk management plan from unauthorized disclosure and modification; system development life cycle procedures; procedures addressing the integration of information security and privacy requirements into the acquisition process; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; list of supply chain threats; list of safeguards to be taken against supply chain threats; system life cycle documentation; inter-organizational agreements and procedures; system security plan; privacy plan; privacy program plan; other relevant documents or records.

Interview: Organizational personnel with acquisition responsibilities; organizational personnel with information security and privacy responsibilities; organizational personnel with supply chain risk management responsibilities.

Test: Organizational processes for defining and documenting the system development life cycle (SDLC); organizational processes for identifying SDLC roles and responsibilities; organizational processes for integrating supply chain risk management into the SDLC; automated mechanisms supporting and/or implementing the SDLC.

SR-02(01): ESTABLISH SCRM TEAM

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization establish a supply chain risk management team consisting of personnel, roles, and responsibilities as identified in the supply chain risk management policy to lead and support the following SCRM activities: supply chain risk management activities as defined in the supply chain risk management plan.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Ensure that all activities are auditable.

SUPPLEMENTAL GUIDANCE

To implement supply chain risk management plans, organizations establish a coordinated, team-based approach to identify and assess supply chain risks and manage these risks by using programmatic and technical mitigation techniques. The team approach enables organizations to conduct an analysis of their supply chain, communicate

with internal and external partners or stakeholders, and gain broad consensus regarding the appropriate resources for SCRM. The SCRM team consists of organizational personnel with diverse roles and responsibilities for leading and supporting SCRM activities, including risk executive, information technology, contracting, information security, privacy, mission, or business, legal, supply chain and logistics, acquisition, business continuity, and other relevant functions.

Members of the SCRM team are involved in various aspects of the SDLC and, collectively, have an awareness of and provide expertise in acquisition processes, legal practices, vulnerabilities, threats, and attack vectors, as well as an understanding of the technical aspects and dependencies of systems. The SCRM team can be an extension of the security and privacy risk management processes or be included as part of an organizational risk management team.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** None. **Federal**: Secure Technology Act; 41 CFR 201; EO 13873; NIST SP 800-30, 800-39, 800-160-1, 800-161; NIST IR 7622, 8272.	CA-2, CP-4, IR-4, MA-2, MA-6, PE-16, PL-2, PM-9, PM-30, RA-3, RA-7, SA-8, SI-4.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Supply chain risk management policy; supply chain risk management procedures; supply chain risk management team charter documentation; supply chain risk management strategy; supply chain risk management implementation plan; procedures addressing supply chain protection; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with acquisition responsibilities; organizational personnel with information security and privacy responsibilities; organizational personnel with supply chain risk management responsibilities; organizational personnel with enterprise risk management responsibilities; legal counsel; organizational personnel with business continuity responsibilities]

SR-03: SUPPLY CHAIN CONTROLS AND PROCESSES

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization establish a supply chain risk management team consisting of personnel, roles, and responsibilities as identified in the supply chain risk management policy to lead and support the following SCRM activities: supply chain risk management activities as defined in the supply chain risk management plan.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Ensure that all activities are auditable.

SUPPLEMENTAL GUIDANCE

To implement supply chain risk management plans, organizations establish a coordinated, team-based approach to identify and assess supply chain risks and manage these risks by using programmatic and technical mitigation techniques. The team approach enables organizations to conduct an analysis of their supply chain, communicate with internal and external partners or stakeholders, and gain broad consensus regarding the appropriate resources for SCRM. The SCRM team consists of organizational personnel with diverse roles and responsibilities for leading and supporting SCRM activities, including risk executive, information technology, contracting, information security, privacy, mission, or business, legal, supply chain and logistics, acquisition, business continuity, and other relevant functions.

Members of the SCRM team are involved in various aspects of the SDLC and, collectively, have an awareness of and provide expertise in acquisition processes, legal practices, vulnerabilities, threats, and attack vectors, as well as an understanding of the technical aspects and dependencies of systems. The SCRM team can be an extension of the security and privacy risk management processes or be included as part of an organizational risk management team.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** None. **Federal**: Secure Technology Act; 41 CFR 201; EO 13873; NIST SP 800-30, 800-39, 800-160-1, 800-161; NIST IR 7622, 8272.	CA-2, CP-4, IR-4, MA-2, MA-6, PE-16, PL-2, PM-9, PM-30, RA-3, RA-7, SA-8, SI-4.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Supply chain risk management policy; supply chain risk management procedures; supply chain risk management strategy; supply chain risk management plan; systems and critical system components inventory documentation; system and services acquisition policy; system and services acquisition procedures; procedures addressing the integration of information security and privacy requirements into the acquisition process; solicitation documentation; acquisition documentation (including purchase orders); service level agreements; acquisition contracts for systems or services; risk register documentation; system security plan; privacy plan; other relevant documents or records

Interview: Organizational personnel with acquisition responsibilities; organizational personnel with information security and privacy responsibilities; organizational personnel with supply chain risk management responsibilities.

Test: Organizational processes for identifying and addressing supply chain element and process deficiencies

SR-04: PROVENANCE

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization documents, monitors, and maintains valid provenance of the following systems, system components, and associated data: all systems and system components under configuration management, and associated data as required by CM-08.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Every system and system component has a point of origin and may be changed throughout its existence. Provenance is the chronology of the origin, development, ownership, location, and changes to a system or system component and associated data. It may also include personnel and processes used to interact with or make modifications to the system, component, or associated data. Organizations consider developing procedures (see SR-01) for allocating responsibilities for the creation, maintenance, and monitoring of provenance for systems and system components; transferring provenance documentation and responsibility between organizations; and preventing and monitoring for unauthorized changes to the provenance records. Organizations have methods to document, monitor, and maintain valid provenance baselines for systems, system components, and related data.

These actions help track, assess, and document any changes to the provenance, including changes in supply chain elements or configuration, and help ensure non-repudiation of provenance information and the provenance change records. Provenance considerations are addressed throughout the system development life cycle and incorporated into contracts and other arrangements, as appropriate.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** None. **Federal**: Secure Technology Act; 41 CFR 201; EO 13873; ISO 27036, 20243; NIST SP 800-160-1, 800-161; NIST IR 7622, 8112, 8272.	CM-8, MA-2, MA-6, RA-9, SA-3, SA-8, SI-4.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Supply chain risk management policy; supply chain risk management procedures; supply chain risk management plan; documentation of critical systems, critical system components, and associated data; documentation showing the history of ownership, custody, and location of and changes to critical systems or critical system components; system architecture; inter-organizational agreements and procedures; contracts; system security plan; privacy plan; personally identifiable information processing policy; other relevant documents or records.

Interview: Organizational personnel with acquisition responsibilities; organizational personnel with information security and privacy responsibilities; organizational personnel with supply chain risk management responsibilities.

Test: Organizational processes for identifying the provenance of critical systems and critical system components; automated mechanisms used to document, monitor, or maintain provenance.

SR-05: ACQUISITION STRATEGIES, TOOLS, AND METHODS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization employs the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: strategies, contract tools, and procurement methods as defined in the supply chain risk management plan.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Use the acquisition/procurement processes to require supply chain entities to implement necessary security safeguards to:

a. Reduce the likelihood of unauthorized modifications at each stage in the supply chain; and

b. Protect information systems and information system components until the agency takes delivery of such systems/components

SUPPLEMENTAL GUIDANCE

The use of the acquisition process provides an important vehicle to protect the supply chain. There are many useful tools and techniques available, including obscuring the end use of a system or system component, using blind or filtered buys, requiring tamper-evident packaging, or using trusted or controlled distribution. The results from a supply chain risk assessment can guide and inform the strategies, tools, and methods that are most applicable to the situation. Tools and techniques may provide protections against unauthorized production, theft, tampering, insertion of counterfeits, insertion of malicious software or backdoors, and poor development practices throughout the system development life cycle. Organizations also consider providing incentives for suppliers who implement controls, promote transparency into their processes and security and privacy practices, provide contract language that addresses the prohibition of tainted or counterfeit components, and restrict purchases from untrustworthy suppliers. Organizations consider providing training, education, and awareness programs for personnel regarding supply chain risk, available mitigation strategies, and when the programs should be employed. Methods for reviewing and protecting development plans, documentation, and evidence are commensurate with the security and privacy requirements of the organization. Contracts may specify documentation protection requirements.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** None. **Federal**: Secure Technology Act; 41 CFR 201; EO 13873; ISO 27036, 20243; NIST SP 800-30, 800-161; NIST IR 7622, 8272; FAR 52.204-25	AT-3, SA-2, SA-3, SA-4, SA-5, SA-8, SA-9, SA-10, SA-15, SR-6, SR-9, SR-10, SR-11.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Supply chain risk management policy; supply chain risk management procedures; supply chain risk management plan; system and services acquisition policy; system and services acquisition procedures; procedures addressing supply chain protection; procedures addressing the integration of information security and privacy requirements into the acquisition process; solicitation documentation; acquisition documentation (including purchase orders); service level agreements; acquisition contracts for systems, system components, or services; documentation of training, education, and awareness programs for personnel regarding supply chain risk; system security plan; privacy plan; other relevant documents or records.

Interview: Organizational personnel with acquisition responsibilities; organizational personnel with information security and privacy responsibilities; organizational personnel with supply chain risk management responsibilities.

Test: Organizational personnel with acquisition responsibilities; organizational personnel with information security and privacy responsibilities; organizational personnel with supply chain risk management responsibilities.

SR-06: SUPPLIER ASSESSMENTS AND REVIEWS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide prior to entering into a contract and annually thereafter.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Ensure that contracts for the purchase of hardware and software using Federal funds comply with all applicable Federal supply chain restrictions including NDAA, FAR, and other regulations.

SUPPLEMENTAL GUIDANCE

An assessment and review of supplier risk includes security and supply chain risk management processes, foreign ownership, control, or influence (FOCI), and the ability of the supplier to effectively assess subordinate second-tier and third-tier suppliers and contractors. The reviews may be conducted by the organization or by an independent third party. The reviews consider documented processes, documented controls, all-source intelligence, and publicly available information related to the supplier or contractor.

Organizations can use open-source information to monitor for indications of stolen information, poor development and quality control practices, information spillage, or counterfeits. In some cases, it may be appropriate or required to share assessment and review results with other organizations in accordance with any applicable rules, policies, or inter-organizational agreements or contracts.

REFERENCES	RELATED CONTROLS

Agency: DFPS Information Security Policy. **State:** None. **Federal**: Secure Technology Act; 41 CFR 201; EO 13873; ISO 27036, 20243; FIPS 140, 180, 186, 202; NIST SP 800-30, 800-161; NIST IR 7622, 8272; FAR 52.204-25.	SR-3, SR-5.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Supply chain risk management policy and procedures; supply chain risk management strategy; supply chain risk management plan; system and services acquisition policy; procedures addressing supply chain protection; procedures addressing the integration of information security requirements into the acquisition process; records of supplier due diligence reviews; system security plan; other relevant documents or records

Interview: Organizational personnel with system and services acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with supply chain protection responsibilities.

Test: Organizational processes for conducting supplier reviews; automated mechanisms supporting and/or implementing supplier reviews.

SR-08: NOTIFICATION AGREEMENTS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the notification of supply chain compromises; results of assessments or audits; and information as defined in Std.01

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Ensure that contracts include specific requirements for provider to notify agency, as applicable, of:

a. End-of-support/End-of-Life;

b. Major changes in a maintenance organization's structure or process (for example, physical move to a

c. different location, change in ownership, outsourcing, or changes in personnel);

d. Successful and attempted threat events that may affect agency's systems;

e. Available protective or mitigating measures to address identified vulnerabilities; and

f. Any system, service, or component-specific information that affects maintenance or continuity plans.

SUPPLEMENTAL GUIDANCE

The establishment of agreements and procedures facilitates communications among supply chain entities. Early notification of compromises and potential compromises in the supply chain that can potentially adversely affect or have adversely affected organizational systems or system components is essential for organizations to effectively respond to such incidents. The results of assessments or audits may include open-source information that contributed to a decision or result and could be used to help the supply chain entity resolve a concern or improve its processes.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** None. **Federal**: Secure Technology Act; 41 CFR 201; EO 13873; ISO 27036; NIST SP 800-30, 800-161; NIST IR 7622.	IR-4, IR-6, IR-8.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Supply chain risk management policy and procedures; supply chain risk management plan; system and services acquisition policy; procedures addressing supply chain protection; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; inter-organizational agreements and procedures; system security plan; other relevant documents or records.

Interview: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with supply chain risk management responsibilities.

Test: Organizational processes for establishing inter-organizational agreements and procedures with supply chain entities.

SR-09: TAMPER RESISTANCE AND DETECTION

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization implements a tamper protection program for the system, system component, or system service.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Protect assets from tampering or unapproved substitution.

Std.02 — Monitor for evidence of tampering indicators.

Std.03 — Prevent security mechanisms from being compromised by adverse physical conditions.

Std.04 — Require authorization for all disabling of tamper detection and response mechanisms.

SUPPLEMENTAL GUIDANCE
Anti-tamper technologies, tools, and techniques provide a level of protection for systems, system components, and services against many threats, including reverse engineering, modification, and substitution. Strong identification combined with tamper resistance and/or tamper detection is essential to protecting systems and components during distribution and when in use.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** None. **Federal**: ISO 20243.	PE-3, PM-30, SA-15, SI-4, SI-7, SR-3, SR-4, SR-5, SR-10, SR-11.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Supply chain risk management policy and procedures; supply chain risk management plan; system and services acquisition policy; procedures addressing supply chain protection; procedures addressing tamper resistance and detection; tamper protection program documentation; tamper protection tools and techniques documentation; tamper resistance and detection tools and techniques documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; system security plan; other relevant documents or records.

Interview: Organizational personnel with tamper protection program responsibilities; organizational personnel with information security responsibilities; organizational personnel with supply chain risk management responsibilities.

Test: Organizational processes for the implementation of the tamper protection program; automated mechanisms supporting and/or implementing the tamper protection program.

SR-09(01): MULTIPLE STAGES OF SYSTEM DEVELOPMENT LIFE CYCLE

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization employs anti-tamper technologies, tools, and techniques throughout the system development life cycle.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

The system development life cycle includes research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal. Organizations use a combination of hardware and software techniques for tamper resistance and detection. Organizations use obfuscation and self-checking to make reverse engineering and modifications more difficult, time-consuming, and expensive for adversaries. The customization of systems and system components can make substitutions easier to detect and therefore limit damage.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** None. **Federal**: ISO 20243.	SA-3.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Supply chain risk management policy and procedures; supply chain risk management plan; system and services acquisition policy; procedures addressing tamper resistance and detection; tamper protection program documentation; tamper protection tools and techniques documentation; tamper resistance and detection tools (technologies) and techniques documentation; system development life cycle documentation; procedures addressing supply chain protection; system development life cycle procedures; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; inter-organizational agreements and procedures; system security plan; other relevant documents or records.

Interview: Organizational personnel with system and services acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with supply chain risk management responsibilities; organizational personnel with SDLC responsibilities.

Test: Organizational processes for employing anti-tamper technologies; automated mechanisms supporting and/or implementing anti-tamper technologies.

SR-10: INSPECTION OF SYSTEMS OR COMPONENTS

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization inspect the following systems or system components: at random; upon receipt and before reassignment; and whenever indicators of compromise are reported to detect tampering: all systems or system components under configuration management.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Examine inconsistencies in tracking and labeling of physical or digital components to identify counterfeit components.

Indications of counterfeit that may be detectable upon delivery include (but are not limited to):

1. Mismatched lot and the date code;
2. Absent or mismatched manufacturer's logo and label on the ICT component and its documentation;
3. Mismatched bar code and printed part number; and
4. Inconsistent descriptions between package materials and datasheet descriptions.

These comparisons can be done via visual inspections, or a variety of pattern-matching techniques used in supply chain logistics. [Source: SP 800-161]

SUPPLEMENTAL GUIDANCE

The inspection of systems or systems components for tamper resistance and detection addresses physical and logical tampering and is applied to systems and system components removed from organization-controlled areas. Indications of a need for inspection include changes in packaging, specifications, factory location, or entity in which the part is purchased, and when individuals return from travel to high-risk locations.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** None. **Federal**: ISO 20243.	AT-3, PM-30, SI-4, SI-7, SR-3, SR-4, SR-5, SR-9, SR-11.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Supply chain risk management policy and procedures; supply chain risk management plan; system and services acquisition policy; records of random inspections; inspection reports/results; assessment reports/results; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; inter-organizational agreements and procedures; system security plan; other relevant documents or records.

Interview: Organizational personnel with system and services acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with supply chain risk management responsibilities.

Test: Organizational processes for establishing inter-organizational agreements and procedures with supply chain entities; organizational processes to inspect for tampering.

SR-11: COMPONENT AUTHENTICITY

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization:

a. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and

b. Report counterfeit system components to source of counterfeit component; approved external reporting organizations; personnel or roles as identified in the supply chain risk management policy.

AGENCY IMPLEMENTATION STANDARDS

None.

SUPPLEMENTAL GUIDANCE

Sources of counterfeit components include manufacturers, developers, vendors, and contractors. Anti-counterfeiting policies and procedures support tamper resistance and provide a level of protection against the introduction of malicious code. External reporting organizations include CISA.

REFERENCES	RELATED CONTROLS
Agency: DFPS Information Security Policy. **State:** None. **Federal**: ISO 20243.	PE-3, SA-4, SI-7, SR-9, SR-10.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Supply chain risk management policy and procedures; supply chain risk management plan; system and services acquisition policy; anti-counterfeit plan; anti-counterfeit policy and procedures; media disposal policy; media protection policy; incident response policy; reports notifying developers, manufacturers, vendors, contractors, and/or external reporting organizations of counterfeit system components; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; inter-organizational agreements and procedures; records of reported counterfeit system components; system security plan; other relevant documents or records.

Interview: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with supply chain risk management responsibilities; organizational personnel with responsibilities for anti-counterfeit policies, procedures, and reporting.

Test: Organizational processes for counterfeit prevention, detection, and reporting; automated mechanisms supporting and/or implementing anti-counterfeit detection, prevention, and reporting.

SR-12: COMPONENT DISPOSAL

Priority: P1

Baseline(s): Low, Moderate, High	Overlay(s): N/A

CONTROL REQUIREMENTS

The organization disposes of system components using the following techniques and methods: techniques and methods in accordance with Stds.01-03.

AGENCY IMPLEMENTATION STANDARDS

Std.01 — Sanitize all components prior to disposal in accordance with MP-06.

Std.02 — Securely dispose of or destroy all components subject to configuration management.

Std.03 — Document all disposals in component inventories.

SUPPLEMENTAL GUIDANCE

Data, documentation, tools, or system components can be disposed of at any time during the system development life cycle (not only in the disposal or retirement phase of the life cycle). For example, disposal can occur during research and development, design, prototyping, or operations/maintenance and include methods such as disk cleaning, removal of cryptographic keys, partial reuse of components. Opportunities for compromise during disposal affect physical and logical data, including system documentation in paper- based or digital files; shipping and delivery documentation; memory sticks with software code; or complete routers or servers that include permanent media, which contain sensitive or proprietary information. Additionally, proper disposal of system components helps to prevent such components from entering the gray market.

REFERENCES	**RELATED CONTROLS**
Agency: DFPS Information Security Policy. **State:** None. **Federal**: ISO 20243.	MP-6.

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Supply chain risk management policy and procedures; supply chain risk management plan; disposal procedures addressing supply chain protection; media disposal policy; media protection policy; disposal records for system components; documentation of the system components identified for disposal; documentation of the disposal techniques and methods employed for system components; system security plan; other relevant documents or records.

Interview: Organizational personnel with system component disposal responsibilities; organizational personnel with information security responsibilities; organizational personnel with supply chain protection responsibilities.

Test: Organizational techniques and methods for system component disposal; automated mechanisms supporting and/or implementing system component disposal

APPENDICES

APPENDIX A: CATALOG FIELDS

DFPS Control ID & Title

Control ID numbers are based on NIST SP 800-53r5, with a leading 0 added for single-digit numbers for ease of sorting.

Baselines

Tailored from NIST SP 800-53B for DFPS systems based on categorization.

Overlays

Tailored from NIST SP 800-53B for DFPS systems processing data based on classification. Note that the Privacy and CJIS overlay are independent of baseline, while the Sensitive overlay is conditional upon baseline.

Requirements

Tailored from SP 800-53 for DFPS systems based on categorization and classification.

Implementation Standards

Developed by DFPS Office of Information Security to ensure requirements are met; treated as requirements for purposes of assessment and included in Requirements field in state-mandated reporting system.

FBI CJIS Security Policy (CSP) version 5.9

Developed by DFPS Office of Information Security to map FBI requirements to the DFPS Catalog.

DFPS References

Agency-specific references.

State References

State-level references including 1 TAC 202.

Federal References

References provided in SP 800-53 or used in control development; formatting may be updated for readability from NIST's provided text or to remove version specifics if not applicable.

Related Controls

Tailored for DFPS from content in SP 800-53r5.

APPENDIX B: CJIS TO DFPS CONTROL IDS		
CSP v5.9 Area	**Requirement**	**NIST SP 800-53 rev. 5 Control**
CJIS Security Policy Area 1 - Information Exchange Agreements		
5.1	Policy Area 1: Information Exchange Agreements	N/A
5.1.1	Information Exchange	AC-21, CA-3, SA-2, SA-4, SA-4(1), SA-12(2), SA-9
5.1.1.1	Information Handling	AC-21, CM-9, CP-6, CP-7, PL-2, PL-7, PL-8, PM-1, IR-8, IR-9, SI-12
5.1.1.2	State and Federal Agency User Agreements	AC-21, CA-3, SA-2, SA-4, SA-4(1), SA-12(2), SA-9
5.1.1.3	Criminal Justice Agency User Agreements	AC-21, CA-3, SA-2, SA-4, SA-4(1), SA-12(2)
5.1.1.4	Inter-Agency and Management Control Agreements	AC-21, CA-3, SA-2, SA-4, SA-4(1), SA-12(2)
5.1.1.5	Private Contractor User Agreements and CJIS Security Addendum	AC-21, CA-3, SA-2, SA-4, SA-4(1), SA-12(2), SA-9
5.1.1.6	Agency User Agreements	AC-21, CA-3, SA-2, SA-4, SA-4(1), SA-12(2), SA-9
5.1.1.7	Outsourcing Standards for Channelers	PE-3, PS-1, PS-2, PS-3, PS-6, PS-7, CA-8
5.1.1.8	Outsourcing Standards for Non-Channelers	AC-21, CA-3, SA-2, SA-4, SA-4(1), SA-12(2), SA-9
5.1.2	Monitoring, Review, and Delivery of Services	RA-3, SA-9, SA-9(1), CA-7
5.1.2.1	Managing Changes to Service Providers	RA-3
5.1.3	Secondary Dissemination	PS-3, PS-6, PS-7
5.1.4	Secondary Dissemination of Non-CHRI CJI	PS-3, PS-6, PS-7
CJIS Security Policy Area 2 - Security Awareness Training		
5.2	Policy Area 2: Security Awareness Training	N/A
5.2.1	Basic Security Awareness Training	AT-1, PL-4, PL-4(1), AT-2, AT-3, IR-2
5.2.1.1	Level One Security Awareness Training	AT-2, AT-3, IR-2, PE-1, PL-4, PL-4(1)
5.2.1.2	Level Two Security Awareness Training	AT-2(2), AT-3, PL-4, PL-4(1), MP-1
5.2.1.3	Level Three Security Awareness Training	AT-2(2), AT-3, PL-4, PL-4(1), C-1, CM-9, CM-10, CM-11, IA-1, PE-1, PS-6
5.2.1.4	Level Four Security Awareness Training	AT-3, CM-10, CM-9, CP-3, IR-2, PS-6
5.2.2	LASO Training	AT-2, AT-3
5.2.3	Security Training Records	AT-4, PL-4
CJIS Security Policy Area 3 - Incident Response		
5.3	Policy Area 3: Incident Response	IR-1, IR-4, IR-5, IR-6, IR-8
5.3.1	Reporting Security Events	IR-4, IR-4(1), IR-4(4), IR-5, IR-5(1), IR-6, IR-6(1) IR-6(2) IR-8, IR-7
5.3.1.1.1	FBI CJIS Division Responsibilities	IR-7, IR-7(1), IR-7(2)
5.3.1.1.2	CSA ISO Responsibilities	IR-1, IR-4, IR-5, IR-6, IR-7, IR-7(2), IR-8
5.3.2	Management of Security Incidents	IR-1, IR-8

5.3.2.1	Incident Handling	IR-4, IR-4(1), IR-4(2), IR-4(3), IR-4(4), IR-5, IR-5(1), AU-6, IR-8
5.3.2.2	Collection of Evidence	AU-6, AU-11, IR-4, IR-4(1), IR-8
5.3.3	Incident Response Training	IR-2, IR-3
5.3.4	Incident Monitoring	IR-5, IR-6, AU-6, AU-9, AU-11
CJIS Security Policy Area 4 - Auditing and Accountability		
5.4	Policy Area 4:Auditing and Accountability	N/A
5.4.1	Auditable Events and Content (Information Systems)	AC-6(9), AC-9, AU-2, AU-2(3), AU-3, AU-3(1), AU-6, AU-6(1), AU-6(3), AU12, CA-2, CA-7, SI-4, AC-2(4)
5.4.1.1	Events	AC-6(9), AC-9, AU-2, AU-12, CA-7, SI-4, AC-2(4), AC-17(1)
5.4.1.1.1	Content	AU-12
5.4.2	Response to Audit Processing Failures	AU-5, AU-5(2)
5.4.3	Audit Monitoring, Analysis, and Reporting	AU-6, AU-6(1), AU-6(3), AU-7, CA-2, CA-7
5.4.4	Time Stamps	AU-8, AU-8(1)
5.4.5	Protection of Audit Information	AU-9, AU-9(4)
5.4.6	Audit Record Retention	AU-4, AU-5(1), AU-9(2), AU-11
5.4.7	Logging NCIC and III Transactions	AU-4, AU-11
CJIS Security Policy Area 5 - Access Control		
5.5	Policy Area 5: Access Control	N/A
5.5.1	Account Management	AC-2, AC-5, IR8, AC-2(1), AC-2(2), AC-2(3), AC-2(4), PS-4
5.5.2	Access Enforcement	AC-2, AC-2(1), AC-2(7), AC-3, AC-3(3), AC-3(4), AC-5, AC-6, AC-6(1), AC6(2), AC-12(1), SC-23(1), SC-23(3)
5.5.2.1	Least Privilege	AC-2, AC-2(4), AC-2(7), AC-5, AC-6, AC-6(5), AC-6(9), AC-10, RA5(5), AC-6(1), AC-6(2)
5.5.2.2	System Access Control	AC-2, AC-2(4), AC-2(7), AC-3, AC-5, AC-6, AC-6(5), AC-6(9), AC-10, RA5(5), AC-2(2)
5.5.2.3	Access Control Criteria	AC-2, AC-2(4), AC-2(7), AC-3, AC-5, AC-6, AC-6(5), AC-6(9), AC-10, RA5(5)
5.5.2.4	Access Control Mechanisms	AC-2, AC-2(4), AC-2(7), AC-3, AC-5, AC-6, AC-6(5), AC-6(9), AC-10, RA5(5), SC-28, AC-4
5.5.3	Unsuccessful Login Attempts	AC-7, IA-5(1)
5.5.4	System Use Notification	AC-8, AC-11(1), AC-22
5.5.5	Session Lock	AC-11, AC-11(1)
5.5.6	Remote Access	AC-17, AC-17(3), AC-17(4), AC-17(6), SI-4, AC-17(1), AC-17(2)
5.5.6.1	Personally Owned Information Systems	AC-17, AC-20
5.5.6.2	Publicly Accessible Computers	AC-17, AC-22
CJIS Security Policy Area 6 - Identification and Authentication		
5.6	Policy Area 6: Identification and Authentication	N/A
5.6.1	Identification Policy and Procedures	IA-1, IA-2, IA-2(5)
5.6.1.1	Use of Originating Agency Identifiers in Transactions and Information Exchanges	SC-16, AC-3, AC-4
5.6.2	Authentication Policy and Procedures	IA-1, IA-2, IA-2(8), IA-2(9), IA-3
5.6.2.1	Standard Authenticators	IA-5, IA-5(1), IA-5(5), IA-6, IA-5(6)
5.6.2.1.1	Password	IA-5, IA-5(1)
5.6.2.1.1.1	Basic Password Standards	IA-5, IA-5(1)
5.6.2.1.1.2	Advanced Password Standards	IA-5, IA-5(1)

5.6.2.1.2	Personal Identification Number (PIN)	IA-5, IA-5(1), IA-2(1), IA-2(2), IA-2(8), IA-2(12
5.6.2.1.3	One-time Passwords (OTP)	A-2 (1), IA-2(2), IA-2(3), IA-2(8), IA-2(11), IA-2(12), IA-5(1), IA-12(4), IA5(5), SC-37, SC-37(1)
5.6.2.2	Advanced Authentication	IA-2(1), IA-2(2), IA-2(3),IA-2(4), IA-2(11), IA-2(13), IA-3(1), IA-5(2), MA-1, MA-4, SC-37, SC-37(1), SC-12
5.6.2.2.1	Advanced Authentication Policy and Rationale	IA-2(1), IA-2(2), IA-2(3),IA-2(4), IA-2(11), IA-3(1), IA-5(2), MA-1, MA-4
5.6.2.2.2	Advanced Authentication Decision Tree	IA-2(1), IA-2(2), IA-2(3),IA-2(4), IA-2(11), IA-3(1), IA-5(2), MA-1, MA-4
5.6.3	Identifier and Authenticator Management	IA-4, IA-4(2), IA-4(4), IA-5, IA-5(8), IA-8, IA-12
5.6.3.1	Identifier Management	AC-2(3), IA-4, IA-4(2), IA-4(4), IA-5(8), IA-8, IA-12, AC-3
5.6.3.2	Authenticator Management	IA-5, IA-5(6), IA-5(8)
5.6.4	Assertions	IA-2(12), IA-8(1), IA-8(2), IA-8(3)
CJIS Security Policy Area 7 - Configuration Management		
5.7	Policy Area 7: Configuration Management	N/A
5.7.1	Access Restrictions for Changes	CM-3, CM-3(2), CM-4, CM-4(2), CM-5(5), CM-5(6), CM-6, CM-9, MA-2, MA5, SA-10, CM-1, PL-1
5.7.1.1	Least Functionality	CM-2, CM-3, CM-6, CM-7, CM-7(1), CM-7(2), CM-7(3), CM-7(4), CM-7(5), CM-8(3), CM-10, CM-11, SA-4(9), SA-9(2)
5.7.1.2	Network Diagram	CA-3, CA-9, SC-7(4), PL-2, PL-8
5.7.2	Security of Configuration Documentation	CM-2, CM-5, CM-5(1), CM-5(2), CM-6, CM-8, CM-8(1), CM-9, SA-4, SA-5, SI-7, CP-9, PL-2
CJIS Security Policy Area 8 - Media Protection		
5.8	Policy Area 8: Media Protection	N/A
5.8.1	Media Storage and Access	AC-20(2), CP-6, CP-7, MA-3(3), MP-2, MP-3, MP-4, SC-28, MP-1
5.8.2	Media Transport	MP-5
5.8.2.1	Digital Media during Transit	MP-5, MP-5(4)
5.8.2.2	Physical Media in Transit	MP-5
5.8.3	Digital Media Sanitization and Disposal	MA-2, MP-6, MP-6(1), MP-6(2), MP-6(3)
5.8.4	Disposal of Physical Media	MP-6
CJIS Security Policy Area 9 - Physical Protection		
5.9	Policy Area 9: Physical Protection	N/A
5.9.1	Physically Secure Location	PE-1
5.9.1.1	Security Perimeter	PE-1, MA-1, MP-1
5.9.1.2	Physical Access Authorizations	MA-4(7), MA-5, PE-2, PE-2(1), PE-3
5.9.1.3	Physical Access Control	CA-8, PE-3, PE-3(3)
5.9.1.4	Access Control for Transmission Medium	PE-4
5.9.1.5	Access Control for Display Medium	PE-5
5.9.1.6	Monitoring Physical Access	CA-8, PE-3, PE-5, PE-6, PE-6(1)
5.9.1.7	Visitor Control	PE-2(3), PE-3
5.9.1.8	Delivery and Removal	PE-2, PE-8, PE-16
5.9.2	Controlled Area	PE-2, PE-5
CJIS Security Policy Area 10 - Systems and Communications Protection and Information Integrity		
5.10	Policy Area 10: System and Communications Protection and Information Integrity	N/A
5.10.1	Information Flow Enforcement	AC-4, AC-20, AC-20(1), CA-3, CA-9, IA-5(7), SC-7(4), SC-7(8), SC-7(11), SC-10, SC-15, SC-15(1)

5.10.1.1	Boundary Protection	AC-20, CA-3(1), CA-3(2), CA-3(5), CA-8, PE-3(2), SC-5, SC-5(1), SC-5(2), SC-7, SC-7(3), SC-7(4), SC-7(5), SC-7(7), SC-7(8), SC-7(11), SC-7(12), SC-7(13), SC-7(14), SC-7(18), SC-24, PE-3
5.10.1.2	Encryption	AC-17(2), IA-7, MA-4(6), SC-8, SC-8(1), SC-8(2), SC-11, SC-12, SC-12(1), SC-12(2), SC-12(3), SC-13, SC-17, SC-28, SC-28(1), SI-7(6)
5.10.1.2.1	Encryption for CJI in Transit	AC-17(2), IA-7, MA-4(6), SC-8, SC-8(1), SC-8(2), SC-11, SC-12, SC-12(1), SC-12(2), SC-13, SC-28, SC-28(1), SI-7(6)
5.10.1.2.2	Encryption for CJI at Rest	AC-17(2), IA-7, SC-12, SC-12(1), SC-12(2), SC-13, SC-28, SC-28(2), SI7(6)
5.10.1.2.3	Public Key Infrastructure (PKI) Technology	IA-2(1), IA-2(2), IA-5(2), IA-5(10), IA-7, IA-8(1), IA-8(5), SC-12(1), SC-12(3), SC-12(4), SC-12(5), SC-13, SC-17, SC-28(2), SI-7(6)
5.10.1.3	Intrusion Detection Tools and Techniques	SC-7(19), SI-4, SI-4(1), SI-4(2), SI-4(4), SI-4(5), SI-4(7), SI-4(9), SI-4(11), SI-4(12), SI-7, SI-7(1), SI-7(7)
5.10.1.4	Voice over Internet Protocol	SC-19
5.10.1.5	Cloud Computing	AC-17, AC-17(1), AC-17(2), AC-17(3), AC-17(4), AC-23, CP-1, CP-2(1), CP-2(3), CP-2(8), CP-6(1), CP-6(3), CP-7, CP-9, CP-10, CP-10(2), IA-1, IA2, IR-1, IR-6, IR-8, IR-9, MA-1, MA-5, MA-5(4), MP-1, MP-2, MP-4, MP-5, MP-6, MP-7, MP-7(1), PE-1, PE-2, PE-3, PE-18, PL-1, PL-2, PL-2(3), PL-4, PL-4(1), PL-7, PL-8, PL-9, PS-1, PS-3, PS-7, SC-2, SC-2(1), SC-3, SC-4, SC-5, SC-5(1), SC-5(2), SC-5(3), SC-6, SC-7, SC-8, SC-9, SC-12, SC-13, SC-13 (1), SC-16, SC-16 (1), SC-20, SC-21, SC-22, SC-23, SC-28, SC-28 (1), SC-28 (2), SC-32, SC-36, SC-38, SC-43, SI-1, SI-13
5.10.2	Facsimile Transmission of CJI	N/A
5.10.3	Partitioning and Virtualization	SC-2, SC-4, AC-3, AC-4
5.10.3.1	Partitioning	SC-2, SC-2(1), SC-3, SC-4, SC-32, AC-3, AC-4, SC-7
5.10.3.2	Virtualization	SC-2, SC-4, SC-3
5.10.4	System and Information Integrity Policy and Procedures	N/A
5.10.4.1	Patch Management	CM-3, CM-4, CM-4(1), CM-8, RA-5, RA-5(1), RA-5(2), RA-5(3), SA-11, SA11(1), SI-2, SI-2(2), SI-2(3), SI-1
5.10.4.2	Malicious Code Protection	AC-6, MA-3(2), MP-7, SI-3, SI-3(1), SI-3(2)
5.10.4.3	Spam and Spyware Protection	SI-8, SI-8(1), SI-8(2)
5.10.4.4	Security Alerts and Advisories	SI-5, SI-5(1), SI-11, IR-8
5.10.4.5	Information Input Restrictions	SI-10, SI-12
CJIS Security Policy Area 11 - Formal Audits		
5.11	Policy Area 11: Formal Audits	N/A
5.11.1	Audits by the FBI CJIS Division	N/A
5.11.1.1	Triennial Compliance Audits by the FBI CJIS Division	CA-2, CA-7, CA-1
5.11.1.2	Triennial Security Audits by the FBI CJIS Division	CA-2, CA-1
5.11.2	Audits by the CSA	CA-2, CA-1
5.11.3	Special Security Inquiries and Audits	CA-2(1), CA-3, CA-5, CA-6, CA-7(1), CM-3(4)
5.11.4	Compliance Subcommittees	N/A, CA-2
CJIS Security Policy Area 12 - Personnel Security		
5.12	Policy Area 12: Personnel Security	N/A
5.12.1	Personnel Screening Requirements for Individuals Requiring Unescorted Access to Unencrypted CJI	PS-2, PS-3, PS-3(1), PS-3(2), PS-3(3), PS-6, PS-6(2), PS-7, PS-1
5.12.2	Personnel Termination	PS-4

5.12.3	Personnel Transfer	PS-5
5.12.4	Personnel Sanctions	PS-8
CJIS Security Policy Area 13 - Mobile Devices		
5.13	Policy Area 13: Mobile Devices	N/A
5.13.1	Wireless Communications Technologies	AC-18, SI-4(14), SI-4(15), AC-1
5.13.1.1	802.11 Wireless Protocols	AC-18(5), SI-4(15), AC-18(1), AC-18(3)
5.13.1.2	Cellular Devices	AC-19, AC-19(5)
5.13.1.2.1	Cellular Service Abroad	AC-19, AC-19(5)
5.13.1.2.2	Voice Transmissions Over Cellular Devices	AC-19, AC-19(5)
5.13.1.3	Bluetooth	AC-18(5)
5.13.1.4	Mobile Hotspots	AC-18, AC-18(1), AC-19, IA-5, IA-5(1), IA-5 (4), SC-40, SI-4(14), SI-4(15)
5.13.2	Mobile Device Management (MDM)	AC-19, AC-19(5), MP-7
5.13.3	Wireless Device Risk Management	AC-19, AC-19(5)
5.13.4	System Integrity	CM-1, CM-2, CM-2(1), CM-2(3), CM-2(7), CM-3, CM-3(1), CM-3(2)
5.13.4.1	Patching/Updates	CM-3, CM-4, CM-4(1), RA-5, RA-5(1), RA-5(2), RA-5(3), SA-11, SA-11(1), SI-2, SI-2(2), SI-2(3)
5.13.4.2	Malicious Code Protection	AC-6, MA-3(2), MP-7, SI-3, SI-3(1), SI-3(2)
5.13.4.3	Personal Firewall	SC-18, SC-18(1), SC-18(2), SC-18(3), SC-18(4), SA-3, SA-8, SA-10
5.13.5	Incident Response	IR-1, IR-2, IR-4, IR-8
5.13.6	Access Control	AC-5, AC-6, AC-6(5), AC-6(9), AC-19, AC-19(5)
5.13.7	Identification and Authentication	IA-1, IA-2, IA-2(1), IA-2(2), IA-2(3), IA-2(4), IA-2(8), IA-2(9), IA-2(11), IA-3, IA-5(2), MA-4, SC-37, SC-37 (1)
5.13.7.1	Local Device Authentication	IA-1, IA-2, IA-2(5), IA-3
5.13.7.2	Advanced Authentication	IA-2(1), IA-2(2), IA-2(3),IA-2(4), IA-2(11), IA-2(13), IA-3(1), IA-5(2), MA-4, SC-37, SC-37(1)
5.13.7.2.1	Compensating Controls	AC-19, IA-3, IA-3(4), PE-18, PE-18(1), PE-20
5.13.7.3	Device Certificates	AC-19, IA-3, IA-3(4)

APPENDIX C: CHANGE LOG

The latest edition of the DFPS Information Security and Privacy Controls Standards Catalog is v1.0, published 02/01/22. The following area is for future changes as new revisions are published.

DFPS Control ID	Section	Change	Date of Change