CALIFORNIA JUDICIAL BRANCH

Information Systems Controls Framework

[JUDICIAL BRANCH ENTITY NAME]

VERSION 2.0

DECEMBER 1, 2018

Table of Contents

1.0 GENERAL

1.1 SCOPE

This framework of information systems controls has been developed for the establishment of a standard security approach within the Judicial Branch of California. In order to produce this framework, input was solicited from multiple courts ranging from small to large in size so that a comprehensive framework could be developed that is suitable to all entities within the judicial branch. This framework is designed to set a direction, identify and address areas of concern expressed by entities within the judicial branch, and to document policies and practices that can assist judicial branch entities with their concerns by providing a framework for creating entity-specific information security policies and procedures.

The goals of this framework are:

- To suggest an overall information security policy, governance and compliance model for judicial branch entities to leverage in building their information security programs including roles, responsibilities, and major activities.
- To provide a holistic information security framework that judicial branch entities can leverage in creating local policies.
- To provide guidance to all members of the judicial branch on the proper handling of sensitive information.
- To provide a basis for security training and educational awareness programs developed by judicial branch entities.
- To provide the basis for the development of implementation standards, procedures, and guidelines for each platform, operating system, application, and security device that can then be monitored and enforced against the policies defined in the framework.

1.2 ORGANIZATIONAL CHARACTERISTICS

The framework establishes how information is to be handled and secured within individual judicial branch entities, how it is exchanged between the judicial branch, local and state justice partners, external third-parties, and with the public. Therefore, security controls (administrative and technical) related to access management are of particular importance.

1.3 DOCUMENTATION STRUCTURE

An information security program is supported by a collection of documentation capturing differing levels of detail while maintaining consistent guidance for all participants. The information security program will consist of the following categories of documents:

- **Organizational Policy** – Expresses management's expectations with regard to security and data protection. Generally limited to identification of base principles, roles and responsibilities, and the security framework. This framework provides the organizational policy for individual judicial branch entities.

- **Implementing Policy** – Further refines management's expectations; usually issued by a subordinate business or organizational unit for the purpose of interpreting the organizational policy to local entity practices. These policies will be developed as needed by the local entity.

- **Standards** – Identify specific hardware and software features and products whose use has been determined to be in support of policy. Standards may be established by local entities as needed to support policy objectives and to streamline operations. Standards require mandatory compliance, are auditable, and grouped by audience, function, or process. A standard outlines a minimum baseline and may be technical or non-technical.

- **Procedures** – Support standards and policy by providing step-by-step instructions for the execution of a security process. Judicial branch entities will develop and document procedures to ensure the quality and repeatability of security processes.

- **Guidelines** – Provide recommendations which can be used when other guidance has not been established. Guidelines are usually created at lower operational levels such as departments to address immediate needs until consensus is reached on broader direction.

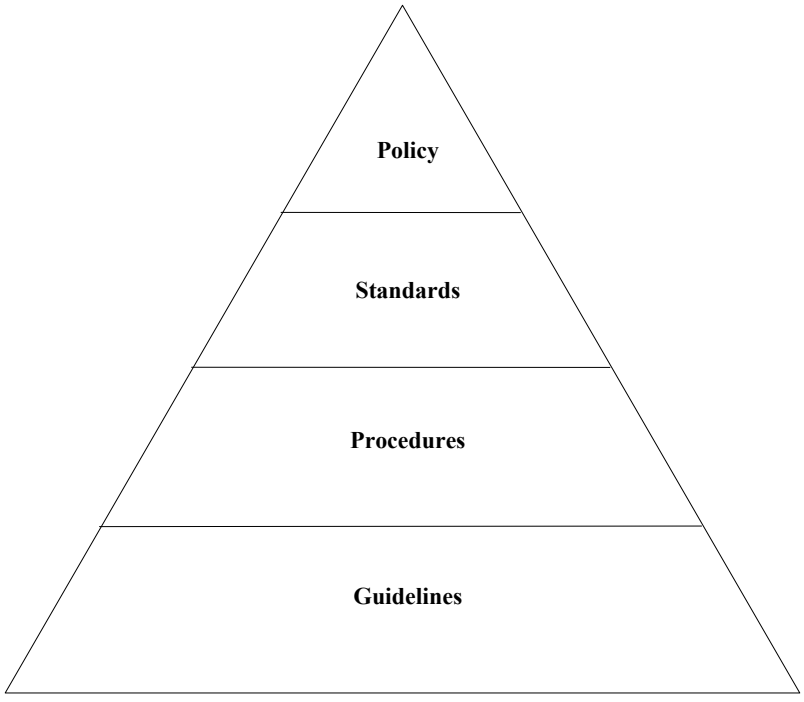


Figure 1: Security Documentation Hierarchy

1.4 FRAMEWORK FORMAT

This framework is structured to align with the National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4 control set to ensure completeness of content and to support future audits. Each chapter generally corresponds to a major family of controls in NIST SP 800-53. The sub-sections identify specific control language, based on the NIST 800-53 set of controls, to be addressed, depending on the baseline impact selection determined by an organizational risk (Please refer to Federal Information Processing Standards (FIPS) Publication 199). For each chapter subsection, the following elements are provided:

- **Control** – Control language adopted from NIST-800-53 Rev. 4 control details
- **Recommendations** – A detailed explanation of recommendations for implementing the control requirements
- **Priority and Baseline Allocation** – A table describing the priority of implementation (P1 – Highest Priority, P2 – Medium Priority, P3 – Lowest Priority), as well as the Baseline alignment with impact ratings (Low: (*NIST Control Ref. No*) Mod: (*NIST Control Ref. No*) High: (*NIST Control Ref. No*))

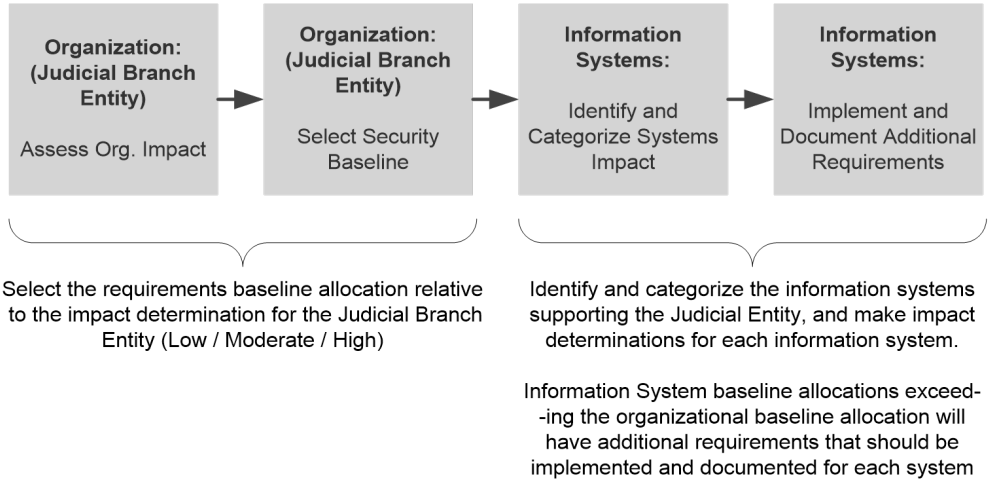
1.5 HOW TO ESTABLISH SECURITY REQUIREMENTS

Security requirements need to be identified so that they may be implemented in support of the judicial branch entity's information security program. In preparation for selecting and specifying the appropriate security requirements for organizational information systems and their respective environments of operation, organizations first determine the criticality and sensitivity of the information to be processed, stored, or transmitted by those systems. This process, known as security categorization, is described in FIPS Publication 199. The security categorization standard is based on a simple and well-established concept—that is, determining the potential adverse impact for organizational information systems. The results of security categorization help guide and inform the selection of appropriate security requirements (i.e., safeguards and countermeasures) to adequately protect those information systems. The security requirements selected for information systems are commensurate with the potential adverse impact on organizational operations and assets, individuals, and other organizations if there is a loss of confidentiality, integrity, or availability. FIPS Publication 199 requires organizations to categorize information systems as low-impact, moderate-impact, or high-impact for the stated security objectives of confidentiality, integrity, and availability (RMF Step 1 - Categorize Information System, NIST 800-37 – '*Guide for Applying the Risk Management Framework to Federal Information Systems*'). The potential impact values assigned to the security objectives are the highest values (i.e., high water mark) from the security categories that have been determined for each type of information processed, stored, or transmitted by those information systems. The generalized format for expressing the security category (SC) of an information system is:

$$\mathbf{SC}_{\text{information system}} = \{(\mathbf{confidentiality}, \textit{impact}), (\mathbf{integrity}, \textit{impact}), (\mathbf{availability}, \textit{impact})\},$$

where the acceptable values for potential impact are low, moderate, or high.

Since the potential impact values for confidentiality, integrity, and availability may not always be the same for a particular information system, the high-water mark concept (introduced in FIPS Publication 199) is used in FIPS Publication 200 to determine the impact level of the information system for the express purpose of selecting the applicable security baseline from one of the three baselines. Thus, a low-impact system is defined as an information system in which all three of the security objectives are low. A moderate-impact system is an information system in which at least one of the security objectives is moderate and no security objective is greater than moderate. Finally, a high-impact system is an information system in which at least one security objective is high. The determination of information system impact levels must be accomplished prior to the consideration of minimum security requirements and the selection of appropriate security controls for those information systems.



Each control contains a table illustrating priority and alignment with the three baselines (Low / Moderate / High). Baselines that do not require the control will be displayed as "None". Baselines with control requirements will display the NIST control reference identifier (i.e. AT-1 in the table would be a reference to Awareness and Training control number 1 in NIST 800-53):

P1	LOW (None /<NIST Ref>)	MOD (None /<NIST Ref>)	HIGH (None /<NIST Ref>)

1.6 DEFINITIONS

For definitions please refer to the Glossary (Appendix B) and Acronyms (Appendix C) of NIST SP 800-53 Rev 4.

2.0 PURPOSE OF INFORMATION SECURITY

Information and the supporting processes, systems, and networks are important assets. Defining, achieving, maintaining, and improving information security may be essential to maintain legal compliance, confidentiality, integrity, and availability of information and systems.

Judicial branch entities and their information systems and networks are faced with security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire or flood. Causes of damage (such as malicious code, computer hacking, and denial of service attacks) have become more common, more ambitious, and increasingly sophisticated.

Many information systems have not been designed with security in mind. The security that can be achieved through technical means is limited and should be supported by appropriate management policies and procedures. Identifying which controls should be in place requires careful planning and attention to detail. Information security management requires, at a minimum, participation by all employees in the branch. It may also require participation from local and state justice partners, the public suppliers, third parties, contract labor, or other external parties.

3.0 INFORMATION SYSTEM CONTROLS

Information is an asset, which, like other important business assets, has value to an organization and consequently needs to be suitably protected. Judicial branch entities, as part of their on-going program to maintain adequate and effective controls, want to ensure that the Information Systems - the devices, operating systems, applications, and the sensitive and confidential information - are adequately protected from the risk of loss due to:

- Intentional acts by third-parties inside or outside the organization.
- Inappropriate access by individuals or groups untrained in correct local policies or procedures.
- Accidental loss of a portable device containing confidential information.
- Accidents, natural disasters, or other force majeure.

Control: Each judicial branch entity shall adopt and maintain:

- An overall security framework, aligned with the National Institute of Standards and Technology (NIST) Special Publication 800-53 rev. 4, to guide staff members responsible for security when implementing information security policies and procedures for the computing platforms and other information assets of the judicial branch entity.
- A basis for security training and educational awareness programs developed by the judicial branch entity.

- IT personnel with the data necessary to convert the security policy contained in this framework to implementation standards for each platform, operating system, application, and security device that can then be monitored and enforced against the policies in the Security Policy Framework (SPF).

The framework shall apply to:

- All desktop computers, servers, data storage devices, communication systems, routers, switches, hubs, mobile devices, and other information system devices owned or leased by the judicial branch entities (the "Computing Platforms").
- Any Computing Platforms, operating system software, middleware, or application software under the control of third parties that connect in any way to our computer or telephone networks.
- All judicial branch entity-owned or leased telephone systems.
- All operating systems and other middleware, which provide the foundation for our Information Systems.
- All proprietary software developed by judicial branch entities or any software developed by a third party specifically for the judicial branch entities.
- All third party "shrink-wrapped" application software licensed by the judicial branch entities and running on any of its Computing Platforms.
- All open-source software legally licensed by the judicial branch entities and running on any of its Computing Platforms.
- Any and all data, information, knowledge, documents, presentations, databases, graphics, or other intellectual property stored on judicial branch entity Computing Platforms.
- All processes and procedures necessary for the protection judicial entity computer platforms.

Persons covered by the framework shall include:

- All full- and part-time employees of the judicial branch entities.
- All exempt and non-exempt employees of the judicial branch entities.
- All independent contractors or other third parties who work on judicial branch entity premises or who remotely connect their Computing Platforms to judicial branch entity Computing Platforms.
- On-Premises and Off-Premises Outsourcing Organizations.

NOTE: Throughout this document, the term 'workforce members' shall include direct employees of the judicial branch entity as well as contractors, vendors, and third parties.

Exceptions to this policy shall be approved by the entity's CIO, leadership committee, Judicial Council, or other designated authority and documented for future review and audit.

4.0 PROGRAM MANAGEMENT

4.1 INFORMATION SECURITY PROGRAM PLAN

Control: The judicial branch entity:

a. Develops and disseminates an entity-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 coordination among judicial branch entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); 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, and individuals, other judicial branch entities, and the State;

b. Reviews the entity-wide information security program plan on an annual basis;

c. Updates the plan to address organizational changes and problems identified during plan implementation or security control assessments; and

d. Protects the information security program plan from unauthorized disclosure and modification.

Recommendations: Information security program plans can be represented in single documents or compilations of documents at the discretion of judicial branch entities. The plans document the program management controls and entity-defined common controls. Information security program plans provide sufficient information about the program management controls/common controls (including specification of parameters for any assignment and selection statements either explicitly or by reference) to enable

implementations that are unambiguously compliant with the intent of the plans and a determination of the risk to be incurred if the plans are implemented as intended.

The security plans for individual information systems and the entity-wide information security program plan together, provide complete coverage for all security controls employed within the local entity. Common controls are to be documented in an appendix to the local entity's information security program plan unless the controls are included in a separate security plan for an information system (e.g., security controls employed as part of an intrusion detection system providing entity-wide boundary protection inherited by one or more organizational information systems). The entity-wide information security program plan will indicate which separate security plans contain descriptions of common controls.

Judicial branch entities have the flexibility to describe common controls in a single document or in multiple documents. In the case of multiple documents, the documents describing common controls are included as attachments to the information security program plan. If the information security program plan contains multiple documents, the local entity specifies in each document the organizational official or officials responsible for the development, implementation, assessment, authorization, and monitoring of the respective common controls. for example, the local entity may require that the Facilities Management Office develop, implement, assess, authorize, and continuously monitor common physical and environmental protection controls from the PE family when such controls are not associated with a particular information system but instead, support multiple information systems.

Priority and Baseline Allocation:

P1	**LOW PM-1**	**MOD PM-1**	**HIGH PM-1**

4.2 SENIOR INFORMATION SECURITY OFFICER

Control: The judicial branch entity appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an entity-wide information security program.

Recommendations: The security officer described in this control is an organizational official. Judicial branch entities may also choose to refer to this official as the Senior Information Security Officer or Chief Information Security Officer.

Priority and Baseline Allocation:

P1	**LOW PM-2**	**MOD PM-2**	**HIGH PM-2**

4.3 INFORMATION SECURITY RESOURCES

Control: The judicial branch entity:

a. Ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement;

b. Employs a business case to record the resources required; and

c. Ensures that information security resources are available for expenditure as planned.

Recommendations: Judicial branch entities consider establishing champions for information security efforts and as part of including the necessary resources, assign specialized expertise and resources as needed. Judicial branch entities may designate and empower an Investment Review Board (or similar group) to manage and provide oversight for the information security-related aspects of the capital planning and investment control process.

Priority and Baseline Allocation:

P1	LOW PM-3	MOD PM-3	HIGH PM-3

4.4 PLAN OF ACTION AND MILESTONES PROCESS

Control: The judicial branch entity:

a. Implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems:

   1. Are developed and maintained;

   2. Document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other judicial branch entities, and the State; and

   3. Are reported in accordance with reporting requirements.

b. Reviews plans of action and milestones for consistency with the organizational risk management strategy and entity-wide priorities for risk response actions.

Recommendations: The plan of action and milestones is a key document in the information security program. With the increasing emphasis on entity-wide risk management across all three tiers in the risk management hierarchy (i.e., local entity, mission/business process, and information system), the local entity must view plans of action and milestones from an organizational perspective, prioritizing risk response actions and ensuring consistency with the goals and objectives of the local entity. Plan of action and milestones updates are based on findings from security control assessments and continuous monitoring activities. OMB FISMA reporting guidance contains instructions regarding organizational plans of action and milestones.

Priority and Baseline Allocation:

P1	**LOW PM-4**	**MOD PM-4**	**HIGH PM-4**

4.5 INFORMATION SYSTEM INVENTORY

Control: The judicial branch entity develops and maintains an inventory of its information systems.

Recommendations: The judicial branch entity identifies all information systems under the control of the entity. The judicial branch entity should identify and document in the inventory the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the entity. The judicial branch entity should review and update the inventory on a [judicial branch entity-defined frequency] basis, made available to the [judicial branch entity-defined recipient], and used to support information resource management. Resource management includes a) information technology planning, budgeting, acquisition, and management, b) monitoring, testing, and evaluation of information security controls.

Priority and Baseline Allocation:

P1	**LOW PM-5**	**MOD PM-5**	**HIGH PM-5**

4.6 INFORMATION SECURITY MEASURES OF PERFORMANCE

Control: The judicial branch entity develops, monitors, and reports on the results of information security measures of performance.

Recommendations: Measures of performance are outcome-based metrics used by the local entity to measure the effectiveness or efficiency of the information security program and the security controls employed in support of the program.

Priority and Baseline Allocation:

P1	**LOW PM-6**	**MOD PM-6**	**HIGH PM-6**

4.7 ENTERPRISE ARCHITECTURE

Control: The judicial branch entity develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other judicial branch entities, and the State.

Recommendations: The enterprise architecture developed by the local entity maintains alignment with the Federal Enterprise Architecture. The integration of information security requirements and associated security controls into the local entity's enterprise architecture helps to ensure that security considerations are addressed early in the system development life cycle and are directly and explicitly related to local mission/business processes. This process of security requirements integration also embeds into the enterprise architecture, an

integral information security architecture consistent with organizational risk management and information security strategies. The Federal Segment Architecture Methodology provides guidance on integrating information security requirements and security controls into enterprise architectures.

Priority and Baseline Allocation:

P1	**LOW PM-7**	**MOD PM-7**	**HIGH PM-7**

4.8 CRITICAL INFRASTRUCTURE PLAN

Control: The judicial branch entity addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

Recommendations: Protection strategies are based on the prioritization of critical assets and resources. Judicial branch entities can identify requirements and obtain guidance for defining critical infrastructure and key resources and for preparing an associated critical infrastructure protection plan from applicable federal and state laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Priority and Baseline Allocation:

P1	**LOW PM-8**	**MOD PM-8**	**HIGH PM-8**

4.9 RISK MANAGEMENT STRATEGY

Control: The judicial branch entity:

a) Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other judicial branch entities, and the State associated with the operation and use of information systems;

b) Implements the risk management strategy consistently across the judicial branch entity; and

c) Reviews and updates the risk management strategy on an annual basis, or as required to address organizational changes.

Recommendations: A judicial branch entity-wide risk management strategy includes, for example, an unambiguous expression of the risk tolerance for the judicial branch entity, acceptable risk assessment methodologies, risk mitigation strategies, a process for consistently evaluating risk across the judicial branch entity with respect to the judicial branch entity's risk tolerance, and approaches for monitoring risk over time. The use of a risk executive function can facilitate consistent, judicial branch entity-wide application of the risk management strategy. The judicial branch entity-wide risk management strategy can be informed by risk-related inputs from other sources both internal and external to the judicial branch entity to ensure the strategy is both broad-based and comprehensive.

Priority and Baseline Allocation:

P1	LOW PM-9	MOD PM-9	HIGH PM-9

4.10 SECURITY AUTHORIZATION PROCESS

Control: The judicial branch entity:

a) Manages (i.e., documents, tracks, and reports) the security state of organizational information systems and the environments in which those systems operate through security authorization processes;

b) Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and

c) Fully integrates the security authorization processes into a judicial branch entity-wide risk management program.

Recommendations: Security authorization processes for information systems and environments of operation require the implementation of a judicial branch entity-wide risk management process, a Risk Management Framework, and associated security standards and guidelines. Specific roles within the risk management process include an organizational risk executive (function) and designated authorizing officials for each organizational information system and common control provider. Security authorization processes are integrated with organizational continuous monitoring processes to facilitate ongoing understanding and acceptance of risk to organizational operations and assets, individuals, other judicial branch entities, and the State.

Priority and Baseline Allocation:

P1	LOW PM-10	MOD PM-10	HIGH PM-10

4.11 MISSION/BUSINESS PROCESS DEFINITION

Control: The judicial branch entity:

a. Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other judicial branch entities, and the State; and

b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until achievable protection needs are obtained.

Recommendations: Information protection needs are technology-independent, required capabilities to counter threats to judicial branch entities, individuals, or the State through the compromise of information (i.e., loss of confidentiality, integrity, or availability).

Information protection needs are derived from the mission/business needs defined by the judicial branch entity, the mission/business processes selected to meet the stated needs, and the organizational risk management strategy. Information protection needs determine the required security controls for the judicial branch entity and the associated information systems supporting the mission/business processes. Inherent in defining a judicial branch entity's information protection needs is an understanding of the level of adverse impact that could result if a compromise of information occurs. The security categorization process is used to make such potential impact determinations. Mission/business process definitions and associated information protection requirements are documented by the judicial branch entity in accordance with organizational policy and procedure.

Priority and Baseline Allocation:

P1	LOW PM-11	MOD PM-11	HIGH PM-11

4.12 INSIDER THREAT PROGRAM

Control: The judicial branch entity implements an insider threat program that includes a cross-discipline insider threat incident handling team.

Recommendations: Judicial branch entities handling classified information are required, under Presidential 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 judicial branch entities 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.

Priority and Baseline Allocation:

P1	LOW PM-12	MOD PM-12	HIGH PM-12

4.13 INFORMATION SECURITY WORKFORCE

Control: The judicial branch entity establishes an information security workforce development and improvement program.

Recommendations: 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) judicial branch entities 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.

Priority and Baseline Allocation:

P1	LOW PM-13	MOD PM-13	HIGH PM-13

4.14 TESTING, TRAINING, AND MONITORING

Control: The judicial branch entity:

a. Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems:

    1. Are developed and maintained; and

    2. Continue to be executed in a timely manner;

b. Reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and judicial branch entity-wide priorities for risk response actions.

Recommendations: This control ensures that judicial branch entities provide oversight for the security testing, training, and monitoring activities conducted judicial branch entity-wide and that those activities are coordinated with the importance of continuous monitoring programs, the implementation of information security across the three tiers of the risk management hierarchy, and the widespread use of common controls, judicial branch entities coordinate and consolidate the testing and monitoring activities that are routinely conducted as part of ongoing organizational assessments supporting a variety of security controls. Security training activities, while typically focused on individual information systems and specific roles, also necessitate coordination across all organizational elements. Testing, training, and monitoring plans and activities are informed by current threat and vulnerability assessments.

Priority and Baseline Allocation:

P1	**LOW PM-14**	**MOD PM-14**	**HIGH PM-14**

4.15 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS

Control: The judicial branch entity establishes and institutionalizes contact with selected groups and associations within the security community:

a. To facilitate ongoing security education and training for organizational personnel;

b. To maintain currency with recommended security practices, techniques, and technologies; and

c. To share current security-related information including threats, vulnerabilities, and incidents.

Recommendations: Ongoing contact with security groups and associations is of paramount importance in an environment of rapidly changing technologies and threats. Security groups and associations include, for example, special interest groups, forums, professional associations, news groups, and/or peer groups of security professionals in similar judicial branch entities. Judicial branch entities select groups and associations based on organizational missions/business functions. Judicial branch entities share threat, vulnerability, and incident information consistent with applicable federal and state laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Priority and Baseline Allocation:

P1	**LOW PM-15**	**MOD PM-15**	**HIGH PM-15**

4.16 THREAT AWARENESS PROGRAM

Control: The judicial branch entity implements a threat awareness program that includes a cross-judicial branch entity information-sharing capability.

Recommendations: 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 judicial branch entities to share threat information. This can include, for example, sharing threat events (i.e., tactics, techniques, and procedures) that judicial branch entities have experienced, mitigations that judicial branch entities 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., judicial branch entities taking part in threat-sharing consortia). Threat information may be highly sensitive requiring special agreements and protection, or less sensitive and freely shared.

Priority and Baseline Allocation:

P1	LOW PM-16	MOD PM-16	HIGH PM-16

5.0 ACCESS CONTROL

5.1 ACCESS CONTROL POLICY AND PROCEDURES

Control: The judicial branch entity:

a. Develops, documents, and disseminates to all workforce members:

   1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the access control policy and associated access controls; and

b. Reviews and updates the current:

   1. Access control policy on an annual basis; and

   2. Access control procedures on an annual basis.

Recommendations: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls in the AC family. Policy and procedures reflect applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the judicial branch entity 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 judicial branch entities or conversely, can be represented by multiple policies reflecting the complex nature of certain judicial branch entities. 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.

Priority and Baseline Allocation:

P1	LOW AC-1	MOD AC-1	HIGH AC-1

5.2 ACCOUNT MANAGEMENT

Control: The judicial branch entity:

a. Identifies and selects the appropriate types of information system accounts required to support organizational missions/business functions.

b. Assigns account managers for information system accounts;

c. Establishes conditions for group and role membership;

d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;

e. Requires approvals by the assigned business owner for requests to create information system accounts;

f. Creates, enables, modifies, disables, and removes information system accounts in accordance with defined procedures or conditions;

g. Monitors the use of information system accounts;

h. Notifies account managers:

   1. When accounts are no longer required;

   2. When users are terminated or transferred; and

   3. When individual information system usage or need-to-know changes;

i. Authorizes access to the information system based on:

   1. A valid access authorization;

   2. Intended system usage; and

   3. Other attributes as required by the judicial branch entity or associated missions/business functions;

j. Reviews accounts for compliance with account management requirements on a quarterly basis; and

k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

Recommendations: Information system account types include, for example, individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service. Some of the account management requirements listed above can be implemented by organizational information systems. The identification of authorized users of the information system and the specification of access privileges reflects the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by appropriate organizational personnel (e.g., system owner, mission/business owner, or chief information security officer) responsible for approving such accounts and privileged access. Judicial branch entities may

choose to define access privileges or other attributes by account, by type of account, or a combination of both. Other attributes required for authorizing access include, for example, restrictions on time-of-day, day-of-week, and point-of-origin. In defining other account attributes, judicial branch entities consider system-related requirements (e.g., scheduled maintenance, system upgrades) and mission/business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements). Failure to consider these factors could affect information system availability. Temporary and emergency accounts are accounts intended for short-term use. Judicial branch entities establish temporary accounts as a part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Judicial branch entities establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts (e.g., local logon accounts used for special tasks defined by judicial branch entities or when network resources are unavailable). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include, for example: (i) when shared/group, emergency, or temporary accounts are no longer required; or (ii) when individuals are transferred or terminated. Some types of information system accounts may require specialized training.

Priority and Baseline Allocation:

P1	**LOW AC-2**	**MOD AC-2 (1) (2) (3) (4)**	**HIGH AC-2 (1) (2) (3) (4) (5) (11) (12) (13)**

5.3 ACCESS ENFORCEMENT

Control: The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

Recommendations: Access control policies (e.g., identity-based policies, role-based policies, control matrices, cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, domains) in information systems. In addition to enforcing authorized access at the information system level and recognizing that information systems can host many applications and services in support of organizational missions and business operations, access enforcement mechanisms can also be employed at the application and service level to provide increased information security.

Priority and Baseline Allocation:

P1	**LOW AC-3**	**MOD AC-3**	**HIGH AC-3**

5.4 INFORMATION FLOW ENFORCEMENT

Control: The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on defined information flow control policies.

Recommendations: 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 judicial branch entity, restricting web requests to the Internet that are not from the internal web proxy server, and limiting information transfers between judicial branch entities based on data structures and content. Transferring information between information systems representing different security domains with different security policies 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. Judicial branch entities 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 regarding mechanisms to reassign security attributes and security labels.

Judicial branch entities 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). Judicial branch entities also consider the trustworthiness of filtering/inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement.

Priority and Baseline Allocation:

P1	LOW AC-4	MOD AC-4	HIGH AC-4

5.5 SEPARATION OF DUTIES

Control: The judicial branch entity:

a. Separates defined duties of individuals;

b. Documents separation of duties of individuals; and

c. Defines information system access authorizations to support separation of duties.

Recommendations: 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, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD AC-5	HIGH AC-5

5.6 LEAST PRIVILEGE

Control: The judicial branch entity employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Recommendations: Judicial branch entities employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Judicial branch entities consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least privilege. Judicial branch entities also apply least privilege to the development, implementation, and operation of organizational information systems.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD AC-6 (1) (2) (5) (9) (10)	HIGH AC-6 (1) (2) (3) (5) (9) (10)

5.7 UNSUCCESSFUL LOGON ATTEMPTS

Control: The information system:

a) Enforces a limit of five (5) consecutive invalid logon attempts by a user during a five (5) hour time period; and

b) Automatically locks the account/node for a five (5) hour period when the maximum number of unsuccessful attempts is exceeded.

Recommendations: This control applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by information systems are usually temporary and automatically release after a predetermined time period established by judicial branch entities. If a delay algorithm is selected, judicial branch entities may choose to employ different algorithms for different information system components based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at both the operating system and the application levels.

Priority and Baseline Allocation:

P2	LOW AC-7	MOD AC-7	HIGH AC-7

5.8 SYSTEM USE NOTIFICATION

Control: The information system:

a. Displays to users a defined system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal and state laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:

   1. Users are accessing a State Government information system;

   2. Information system usage may be monitored, recorded, and subject to audit;

   3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and

   4. Use of the information system indicates consent to monitoring and recording;

b. Retains 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 information system; and

c. for publicly accessible systems:

   1. Displays system use information before granting further access;

   2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and

3. Includes a description of the authorized uses of the system.

Recommendations: 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. Judicial branch entities should consider system use notification messages/banners displayed in multiple languages based on specific organizational needs and the demographics of information system users. Entities also consult with the Office of the General Counsel for legal review and approval of warning banner content.

Priority and Baseline Allocation:

P1	LOW AC-8	MOD AC-8	HIGH AC-8

5.9 CONCURRENT SESSION CONTROL

Control: The information system limits the number of concurrent sessions for defined accounts and/or account types to a defined limit.

Recommendations: Judicial branch entities may define the maximum number of concurrent sessions for information system accounts globally, by account type (e.g., privileged user, non-privileged user, domain, specific application), by account, or a combination. For example, entities may limit the number of concurrent sessions for system administrators or individuals working in particularly sensitive domains or mission-critical applications. This control addresses concurrent sessions for information system accounts and does not address concurrent sessions by single users via multiple system accounts.

Priority and Baseline Allocation:

P3	LOW Not Selected	MOD Not Selected	HIGH AC-10

5.10 SESSION LOCK

Control: The information system:

a. Prevents further access to the system by initiating a session lock after a thirty (30) minutes of inactivity or upon receiving a request from a user; and

b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

Recommendations: Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of information systems but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined. This is typically at the operating system level but can also be at the application level. Session locks are not an acceptable substitute for logging out

of information systems, for example, if judicial branch entities require users to log out at the end of workdays.

Priority and Baseline Allocation:

P3	**LOW Not Selected**	**MOD AC11 (1)**	**HIGH AC-11 (1)**

5.11 SESSION TERMINATION

Control: The information system automatically terminates a user session after defined conditions or trigger events requiring session disconnect.

Recommendations: This control addresses the termination of user-initiated logical sessions. 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 information system. Such user sessions can be terminated (and thus terminate user access) without terminating network sessions. Session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events requiring automatic session termination can include, for example, judicial branch entity-defined periods of user inactivity, targeted responses to certain types of incidents, time-of-day restrictions on information system use.

Priority and Baseline Allocation:

P2	**LOW Not Selected**	**MOD AC-12**	**HIGH AC-12**

5.12 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

Control: The judicial branch entity:

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

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

Recommendations: This control addresses situations in which judicial branch entities determine that no identification or authentication is required in organizational information systems. Judicial branch entities may allow a limited number of user actions without identification or authentication including, for example, when individuals access public websites or other publicly accessible federal information systems, when individuals use mobile phones to receive calls, or when facsimiles are received. Judicial branch entities also identify actions that normally require identification or authentication but may under certain circumstances (e.g., emergencies), 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. This control 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. Judicial branch entities may decide that there are no user actions that can be performed on organizational information systems without identification and authentication and thus, the values for assignment statements can be *none*.

Priority and Baseline Allocation:

P3	LOW AC-14	MOD AC-14	HIGH AC-14

5.13 REMOTE ACCESS

Control: The judicial branch entity:

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.

Recommendations: 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. Judicial branch entities 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 judicial branch entity 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 judicial branch entities 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.

Priority and Baseline Allocation:

P1	LOW AC-17	MOD AC-17	HIGH AC-17

5.14 WIRELESS ACCESS

Control: The judicial branch entity:

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

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

Recommendations: Wireless technologies include, for example, microwave, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., EAP/TLS, PEAP), which provide credential protection and mutual authentication.

Priority and Baseline Allocation:

P1	LOW AC-18	MOD AC-18 (1)	HIGH AC-18 (1) (4) (5)

5.15 ACCESS CONTROL FOR MOBILE DEVICES

Control: The judicial branch entity:

a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for judicial branch entity-controlled mobile devices; and

b. Authorizes the connection of mobile devices to organizational information systems.

Recommendations: 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). Judicial branch entities 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.

Priority and Baseline Allocation:

P1	LOW AC-19	MOD AC-19 (5)	HIGH AC-19 (5)

5.16 USE OF EXTERNAL INFORMATION SYSTEMS

Control: The judicial branch entity establishes terms and conditions, consistent with any trust relationships established with other judicial branch entities and/or any external organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

a. Access the information system from external information systems; and

b. Process, store, or transmit judicial branch entity-controlled information using external information systems.

Recommendations: External information systems are information systems or components of information systems that are outside of the authorization boundary established by judicial branch entities and for which judicial branch entities typically have no direct supervision and authority over the application of required security controls or the assessment of control effectiveness. External information systems include, for example: (i) personally owned information systems/devices (e.g., notebook computers, smart phones, tablets, personal digital assistants); (ii) privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, train stations, convention centers, shopping malls, or airports); (iii) information systems owned or controlled by non-judicial branch entities; and (iv) judicial branch systems that are not owned by, operated by, or under the direct supervision and authority of judicial branch entities. This control also addresses the use of external information systems for the processing, storage, or transmission of organizational information, including, for example, accessing cloud services (e.g., infrastructure as a service, platform as a service, or software as a service) from organizational information systems.

For some external information systems (i.e., information systems operated by other judicial branch entities) the trust relationships that have been established between those judicial branch entities and the originating judicial branch entity may be such, that no explicit terms and conditions are required. Information systems within these judicial branch entities would not be considered external. These situations occur when, for example, there are pre-existing sharing/trust agreements (either implicit or explicit) established between t judicial branch

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

This control does not apply to the use of external information systems to access public interfaces to organizational information systems (e.g., individuals accessing Judicial Branch information through www.courts.ca.gov). Judicial branch entities establish terms and conditions for the use of external information systems in accordance with organizational security policies and procedures. Terms and conditions address as a minimum: types of applications that can be accessed on organizational information systems from external information systems; and the highest security category of information that can be processed, stored, or transmitted on external information systems. If terms and conditions with the owners of external information systems cannot be established, judicial branch entities may impose restrictions on organizational personnel using those external systems.

Priority and Baseline Allocation:

P1	**LOW AC-20**	**MOD AC-20 (1) (2)**	**HIGH AC-20 (1) (2)**

5.17 INFORMATION SHARING

Control: The judicial branch entity:

a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for defined information sharing circumstances where user discretion is required; and

b. Employs defined automated mechanisms or manual processes to assist users in making information sharing/collaboration decisions.

Recommendations: This control applies to information that may be restricted in some manner (e.g., privileged medical information, contract-sensitive information, proprietary information, personally identifiable information, classified information related to special access programs or compartments) based on some formal or administrative determination. Depending on the particular information-sharing 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/compartment.

Priority and Baseline Allocation:

P2	**LOW Not Selected**	**MOD AC-21**	**HIGH AC-21**

5.18 PUBLICLY ACCESSIBLE CONTENT

Control: The judicial branch entity:

a. Designates individuals authorized to post information onto a publicly accessible information system;

b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

c. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and

d. Reviews the content on the publicly accessible information system for nonpublic information on a monthly basis and removes such information, if discovered.

Recommendations: In accordance with federal and state laws, Executive Orders, directives, policies, regulations, standards, and/or guidance, the general public is not authorized access to nonpublic information (e.g., information protected under the Privacy Act and proprietary information). This control addresses information systems that are controlled by the judicial branch entity and accessible to the general public, typically without identification or authentication. The posting of information on non-judicial branch entity information systems is covered by organizational policy.

Priority and Baseline Allocation:

P3	LOW AC-22	MOD AC-22	HIGH AC-22

6.0 AWARENESS AND TRAINING

6.1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES

Control: The judicial branch entity:

a. Develops, documents, and disseminates to all workforce members:

   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 updates the current:

   1. Security awareness and training policy on an annual basis; and

   2. Security awareness and training procedures on an annual basis.

Recommendations: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls in the AT family. Policy and procedures reflect applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the judicial branch entity 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 judicial branch entities or conversely, can be represented by multiple policies reflecting the complex nature of certain judicial branch entities. 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.

Priority and Baseline Allocation:

P1	LOW AT-1	MOD AT-1	HIGH AT-1

6.2 SECURITY AWARENESS TRAINING

Control: The judicial branch entity provides basic security awareness training to information system users (including managers, senior executives, and contractors):

a. As part of initial training for new users;

a. When required by information system changes; and

b. Annually thereafter.

Recommendations: Judicial branch entities determine the appropriate content of security awareness training and security 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 to respond to suspected security incidents. The content also addresses awareness of the need for operations security. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events.

Priority and Baseline Allocation:

P1	LOW AT-2	MOD AT-2 (2)	HIGH AT-2 (2)

6.3 ROLE-BASED SECURITY TRAINING

Control: The judicial branch entity provides role-based security training to personnel with assigned security roles and responsibilities:

a. Before authorizing access to the information system or performing assigned duties;

b. When required by information system changes; and

c. Annually thereafter.

Recommendations: Judicial branch entities determine the appropriate content of security training based on the assigned roles and responsibilities of individuals and the specific security requirements of judicial branch entities and the information systems to which personnel have authorized access. In addition, judicial branch entities 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. Judicial branch entities also provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of organizational information security programs. Role-based security training also applies to contractors providing services to federal agencies.

Priority and Baseline Allocation:

P1	LOW AT-3	MOD AT-3	HIGH AT-3

6.4 SECURITY TRAINING RECORDS

Control: The judicial branch entity:

a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and

b. Retains individual training records for five (5) years.

Recommendations: Documentation for specialized training may be maintained by individual supervisors at the option of the judicial branch entity.

Priority and Baseline Allocation:

P3	LOW AT-4	MOD AT-4	HIGH AT-4

7.0 AUDIT AND ACCOUNTABILITY

7.1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

Control: The judicial branch entity:

a. Develops, documents, and disseminates to all workforce members:

   1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and

b. Reviews and updates the current:

   1. Audit and accountability policy on an annual basis; and

   2. Audit and accountability procedures on an annual basis.

Recommendations: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls in the AU family. Policy and procedures reflect applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the judicial branch entity 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 judicial branch entities or conversely, can be represented by multiple policies reflecting the complex nature of certain judicial branch entities. 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.

Priority and Baseline Allocation:

P1	LOW AU-1	MOD AU-1	HIGH AU-1

7.2 AUDIT EVENTS

Control: The judicial branch entity:

a. Determines that the information system is capable of auditing judicial branch entity defined events.

b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;

c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and

d. Determines that the following events are to be audited within the information system: a subset of the judicial branch entity defined events defined in 'Audit Events (a)' (or AU-2(a)) along with the defined frequency of (or situation requiring) auditing for each identified event.

Recommendations: An event is any observable occurrence in an organizational information system. Judicial branch entities identify audit events as those events which are significant and relevant to the security of information systems and the environments in which those systems operate in order to meet specific and ongoing audit needs. Audit events can include, for example, password changes, failed logons, or failed accesses related to information systems, administrative privilege usage, PIV credential usage, or third-party credential usage. In determining the set of auditable events, judicial branch entities consider the auditing appropriate for each of the security controls to be implemented to balance auditing requirements with other information system needs, this control also requires identifying that subset of auditable events that are audited at a given point in time. For example, judicial branch entities may determine that information systems must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance. Auditing requirements, including the need for auditable events, may be referenced in other security controls. Judicial branch entities also include auditable events that are required by applicable federal and state laws, Executive Orders, directives, policies, regulations, and standards. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the appropriate level of abstraction is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Judicial branch entities consider in the definition of auditable events, the auditing necessary to cover related events such as the steps in distributed, transaction-based processes (e.g., processes that are distributed across multiple judicial branch entities) and actions that occur in service-oriented architectures.

Priority and Baseline Allocation:

P1	LOW AU-2	MOD AU-2 (3)	HIGH AU-2 (3)

7.3 CONTENT OF AUDIT RECORDS

Control: The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred,

the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

Recommendations: Audit record content that may be necessary to satisfy the requirement of this control, includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked. Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the information system after the event occurred).

Priority and Baseline Allocation:

P1	LOW AU-3	MOD AU-3 (1)	HIGH AU-3 (1) (2)

7.4 AUDIT STORAGE CAPACITY

Control: The judicial branch entity allocates audit record storage capacity in accordance with defined audit record storage requirements.

Recommendations: Judicial branch entities consider the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity. Allocating sufficient audit storage capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of auditing capability.

Priority and Baseline Allocation:

P1	LOW AU-4	MOD AU-4	HIGH AU-4

7.5 RESPONSE TO AUDIT PROCESSING FAILURES

Control: The information system:

a. Alerts judicial branch entity-defined personnel or roles in the event of an audit processing failure; and

b. Takes the following additional actions: stop generating audit records.

Recommendations: Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Judicial branch entities may choose to define additional actions for different audit processing failures (e.g., by type, by location, by severity, or a combination of such factors). This control applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the total audit storage capacity of judicial branch entities (i.e., all audit data storage repositories combined), or both.

Priority and Baseline Allocation:

P1	LOW AU-5	MOD AU-5	HIGH AU-5 (1) (2)

7.6 AUDIT REVIEW, ANALYSIS, AND REPORTING

Control: The judicial branch entity:

a. Reviews and analyzes information system audit records on a monthly basis for indications of inappropriate or unusual activity; and

b. Reports findings to the system owner, business/information owner, and CSO, as necessary and appropriate.

Recommendations: Audit review, analysis, and reporting covers information security-related auditing performed by judicial branch entities including, for example, auditing that results from monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and nonlocal maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at the information system boundaries, use of mobile code, and use of VoIP. Findings can be reported to organizational entities that include, for example, incident response team, help desk, information security group/department. If judicial branch entities are prohibited from reviewing and analyzing audit information or unable to conduct such activities (e.g., in certain national security applications or systems), the review/analysis may be carried out by other judicial branch entities granted such authority.

Priority and Baseline Allocation:

P1	LOW AU-6	MOD AU-6 (1) (3)	HIGH AU-6 (1) (3) (5) (6)

7.7 AUDIT REDUCTION AND REPORT GENERATION

Control: 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 ordering of audit records.

Recommendations: Audit reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to analysts. Audit reduction and report generation capabilities do not always emanate from the same information system or from the same organizational entities conducting auditing activities. Audit reduction capability can include, for example, modern data mining techniques with advanced data filters to identify anomalous behavior in audit records. The report generation capability provided by the information system can generate customizable reports. Time ordering of audit records can be a significant issue if the granularity of the timestamp in the record is insufficient.

Priority and Baseline Allocation:

P2	LOW Not Selected	MOD AU-7 (1)	HIGH AU-7 (1)

7.8 TIME STAMPS

Control: The information system:

a. Uses internal system clocks to generate time stamps for audit records; and

b. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets a defined granularity of time measurement.

Recommendations: 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. Judicial branch entities 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.

Priority and Baseline Allocation:

P1	LOW AU-8	MOD AU-8 (1)	HIGH AU-8 (1)

7.9 PROTECTION OF AUDIT INFORMATION

Control: The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

Recommendations: Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity. This control focuses on technical protection of audit information. Physical protection of audit information is addressed by media protection controls and physical and environmental protection controls.

Priority and Baseline Allocation:

P1	LOW AU-9	MOD AU-9 (4)	HIGH AU-9 (2) (3) (4)

7.10 NON-REPUDIATION

Control: The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed defined actions to be covered by non-repudiation.

Recommendations: Types of individual actions covered by non-repudiation include, for example, creating information, sending and receiving messages, approving information (e.g., indicating concurrence or signing a contract). Non-repudiation protects individuals against later claims by: (i) authors of not having authored particular documents; (ii) senders of not having transmitted messages; (iii) receivers of not having received messages; or (iv) signatories of not having signed documents. Non-repudiation services can be used to determine if information originated from a particular individual, or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request) or received specific information. Judicial branch entities obtain non-repudiation services by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts).

Priority and Baseline Allocation:

P2	LOW Not Selected	MOD Not Selected	HIGH AU-10

7.11 AUDIT RECORD RETENTION

Control: The judicial branch entity retains audit records for a defined time period consistent with records retention policy to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Recommendations: Judicial branch entities retain audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoenas, and law enforcement actions. Judicial branch entities 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 record retention.

Priority and Baseline Allocation:

P3	LOW AU-11	MOD AU-11	HIGH AU-11

7.12 AUDIT GENERATION

Control: The information system:

a. Provides audit record generation capability for the auditable events at in ‘Audit Events (a)’ (or AU-2(a)) at defined information system components;

b. Allows judicial branch entity-defined personnel or roles to select which auditable events are to be audited by specific components of the information system; and

c. Generates audit records for the events defined in ‘Audit Events (d)’ with content defined in ‘Content of Audit Records’.

Recommendations: Audit records can be generated from many different information system components. The list of audited events is the set of events for which audits are to be generated. These events are typically a subset of all events for which the information system is capable of generating audit records.

Priority and Baseline Allocation:

P1	**LOW AU-12**	**MOD AU-12**	**HIGH AU-12 (1) (3)**

8.0 SECURITY ASSESSMENT AND AUTHORIZATION

8.1 SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES

Control: The judicial branch entity:

a. Develops, documents, and disseminates to workforce members:

   1. A security assessment and authorization 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 assessment and authorization policy and associated security assessment and authorization controls; and

b. Reviews and updates the current:

   1. Security assessment and authorization policy on an annual basis; and

   2. Security assessment and authorization procedures on an annual basis.

Recommendations: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls in the CA family. Policy and procedures reflect applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the judicial branch entity 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 judicial branch entities or conversely, can be represented by multiple policies reflecting the complex nature of certain judicial branch entities. 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.

Priority and Baseline Allocation:

P1	LOW CA-1	MOD CA-1	HIGH CA-1

8.2 SECURITY ASSESSMENTS

Control: The judicial branch entity:

a. Develops a security assessment plan that describes the scope of the assessment including:

   1. Security controls under assessment;

2. Assessment procedures to be used to determine security control effectiveness; and

3. Assessment environment, assessment team, and assessment roles and responsibilities;

b. Assesses the security controls in the information system and its environment of operation on a two (2) year basis 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 requirements;

c. Produces a security assessment report that documents the results of the assessment; and

d. Provides the results of the security control assessment to judicial branch entity-defined individuals or roles responsible for the information systems/processes within scope of the assessment.

Recommendations: Judicial branch entities assess security controls in organizational information systems and the environments in which those systems operate as part of: (i) initial and ongoing security authorizations; (ii) FISMA annual assessments; (iii) continuous monitoring; and (iv) system development life cycle activities. Security assessments: (i) ensure that information security is built into organizational information systems; (ii) identify weaknesses and deficiencies early in the development process; (iii) provide essential information needed to make risk-based decisions as part of security authorization processes; and (iv) ensure compliance to vulnerability mitigation procedures. Assessments are conducted on the implemented security controls from Appendix F (main catalog) and Appendix G (Program Management controls) as documented in System Security Plans and Information Security Program Plans. Judicial branch entities can use other types of assessment activities such as vulnerability scanning and system monitoring to maintain the security posture of information systems during the entire life cycle. Security assessment reports document assessment results in sufficient detail as deemed necessary by judicial branch entities, to determine the accuracy and completeness of the reports and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements. Security assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted. For example, assessments conducted in support of security authorization decisions are provided to authorizing officials or authorizing official designated representatives.

To satisfy annual assessment requirements, judicial branch entities can use assessment results from the following sources: (i) initial or ongoing information system authorizations; (ii) continuous monitoring; or (iii) system development life cycle activities. Judicial branch entities ensure that security assessment results are current, relevant to the determination of security control effectiveness, and obtained with the appropriate level of assessor independence. Existing security 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. Subsequent to initial authorizations and in accordance with judicial branch entity policy, judicial branch entities assess security controls during continuous monitoring. Judicial branch entities establish the frequency for ongoing security control assessments in accordance with organizational continuous monitoring strategies. Information Assurance Vulnerability Alerts provide useful examples of vulnerability mitigation procedures. External audits (e.g., audits by external entities such as regulatory agencies) are outside the scope of this control.

Priority and Baseline Allocation:

P2	LOW CA-2	MOD CA-2 (1)	HIGH CA-2 (1) (2)

8.3 SYSTEM INTERCONNECTIONS

Control: The judicial branch entity:

a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements;

b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and

c. Reviews and updates Interconnection Security Agreements on an annual basis.

Recommendations: This control applies to dedicated connections between information systems (i.e., system interconnections) and does not apply to transitory, user-controlled connections such as email and website browsing. Judicial branch entities carefully consider the risks that may be introduced when information systems are connected to other systems with different security requirements and security controls, both within judicial branch entities and external to judicial branch entities. Authorizing officials determine the risk associated with information system connections and the appropriate controls employed. If interconnecting systems have the same authorizing official, judicial branch entities do not need to develop Interconnection Security Agreements. Instead, judicial branch entities can describe the interface characteristics between those interconnecting systems in their respective security plans. If interconnecting systems have different authorizing officials within the same judicial branch entity, judicial branch entities can either develop Interconnection Security Agreements or describe the interface characteristics between systems in the security plans for the respective systems. Judicial branch entities may also incorporate Interconnection Security Agreement information into formal contracts, especially for interconnections established between federal agencies and nonfederal (i.e., private sector) Judicial Branch Entities. Risk considerations also include information systems sharing the same networks. For certain technologies (e.g., space, unmanned aerial vehicles, and medical devices), there may be specialized connections in place during

preoperational testing. Such connections may require Interconnection Security Agreements and be subject to additional security controls.

Priority and Baseline Allocation:

P1	LOW CA-3	MOD CA-3 (5)	HIGH CA-3 (5)

8.4 PLAN OF ACTION AND MILESTONES

Control: The judicial branch entity:

a. Develops a plan of action and milestones for the information system to document the judicial branch entity's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and

b. Updates existing plan of action and milestones on a two (2) year basis based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

Recommendations: Plans of action and milestones are key documents in security authorization packages.

Priority and Baseline Allocation:

P3	LOW CA-5	MOD CA-5	HIGH CA-5

8.5 SECURITY AUTHORIZATION

Control: The judicial branch entity:

a. Assigns a senior-level executive or manager as the authorizing official for the information system;

b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and

c. Updates the security authorization on a three (3) year basis.

Recommendations: Security authorizations are official management decisions, conveyed through authorization decision documents, by senior organizational officials or executives (i.e., authorizing officials) to authorize operation of information systems and to explicitly accept the risk to organizational operations and assets, individuals, other judicial branch entities, and the State based on the implementation of agreed-upon security controls. Authorizing officials provide budgetary oversight for organizational information systems or assume responsibility for the mission/business operations supported by those systems. The security authorization process is an inherently judicial branch responsibility and therefore,

authorizing officials must be judicial branch employees. Through the security authorization process, authorizing officials assume responsibility and are accountable for security risks associated with the operation and use of organizational information systems. Accordingly, authorizing officials are in positions with levels of authority commensurate with understanding and accepting such information security-related risks. Continuous monitoring programs can satisfy three-year reauthorization requirements, so separate reauthorization processes are not necessary. Through the employment of comprehensive continuous monitoring processes, critical information contained in authorization packages (i.e., security plans, security assessment reports, and plans of action and milestones) is updated on an ongoing basis, providing authorizing officials and information system owners with an up-to-date status of the security state of organizational information systems and environments of operation. to reduce the administrative cost of security reauthorization, authorizing officials use the results of continuous monitoring processes to the maximum extent possible as the basis for rendering reauthorization decisions.

Priority and Baseline Allocation:

P2	LOW CA-6	MOD CA-6	HIGH CA-6

8.6 CONTINUOUS MONITORING

Control: The judicial branch entity develops a continuous monitoring strategy and implements a continuous monitoring program that includes:

a. Establishment of defined metrics to be monitored;

b. Establishment of defined frequencies for monitoring and defined frequencies for assessments supporting such monitoring;

c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;

d. Ongoing security status monitoring of judicial branch entity-defined metrics in accordance with the organizational continuous monitoring strategy;

e. Correlation and analysis of security-related information generated by assessments and monitoring;

f. Response actions to address results of the analysis of security-related information; and

g. Reporting the security status of judicial branch entity and the information system to the CSO, business/information owner, and system owner on an annual basis.

Recommendations: Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The terms continuous and ongoing imply that judicial branch entities

assess/analyze security controls and information security-related risks at a frequency sufficient to support organizational risk-based decisions. The results of continuous monitoring programs generate appropriate risk response actions by judicial branch entities. Continuous monitoring programs also allow judicial branch entities to maintain the security authorizations of information systems and common controls over time in highly dynamic environments of operation with changing mission/business needs, threats, vulnerabilities, and technologies. Having access to security-related information on a continuing basis through reports/dashboards gives organizational officials the capability to make more effective and timely risk management decisions, including ongoing security authorization decisions. Automation supports more frequent updates to security authorization packages, hardware/software/firmware inventories, 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 information systems.

Priority and Baseline Allocation:

P2	LOW CA-7	MOD CA-7 (1)	HIGH CA-7 (1)

8.7 PENETRATION TESTING

Control: The judicial branch entity conducts penetration testing on an annual basis on defined information systems or system components.

Recommendations: Penetration testing is a specialized type of assessment conducted on information systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Such testing can be used to either validate vulnerabilities or determine the degree of resistance organizational information systems have to adversaries within a set of specified constraints (e.g., time, resources, and/or skills). Penetration testing attempts to duplicate the actions of adversaries in carrying out hostile cyber-attacks against judicial branch entities and provides a more in-depth analysis of security-related weaknesses/deficiencies. Judicial branch entities can also use the results of vulnerability analyses to support penetration testing activities. Penetration testing can be conducted on the hardware, software, or firmware components of an information system and can exercise both physical and technical security controls. A standard method for penetration testing includes, for example: (i) pretest analysis based on full knowledge of the target system; (ii) pretest identification of potential vulnerabilities based on pretest analysis; and (iii) testing designed to determine exploitability of identified vulnerabilities. All parties agree to the rules of engagement before the commencement of penetration testing scenarios. Judicial branch entities correlate the penetration testing rules of engagement with the tools, techniques, and procedures that are anticipated to be employed by adversaries carrying out attacks. Organizational risk assessments guide decisions on the level of independence required for personnel conducting penetration testing.

Priority and Baseline Allocation:

P2	**LOW Not Selected**	**MOD Not Selected**	**HIGH CA-8**

8.8 INTERNAL SYSTEM CONNECTIONS

Control: The judicial branch entity:

a. Authorizes internal connections of defined information system components or classes of components to the information system; and

b. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

Recommendations: This control applies to connections between organizational information systems and (separate) constituent system components (i.e., intra-system connections) including, for example, system connections with mobile devices, notebook/desktop computers, printers, copiers, facsimile machines, scanners, sensors, and servers. Instead of authorizing each individual internal connection, judicial branch entities can authorize internal connections for a class of components with common characteristics and/or configurations, for example, all digital printers, scanners, and copiers with a specified processing, storage, and transmission capability or all smart phones with a specific baseline configuration.

Priority and Baseline Allocation:

P2	**LOW CA-9**	**MOD CA-9**	**HIGH CA-9**

9.0 CONFIGURATION MANAGEMENT

9.1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES

Control: The judicial branch entity:

a. Develops, documents, and disseminates to all workforce members:

   1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and

b. Reviews and updates the current:

   1. Configuration management policy on an annual basis; and

   2. Configuration management procedures on an annual basis.

Recommendations: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls in the CM family. Policy and procedures reflect applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the judicial branch entity 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 judicial branch entities or conversely, can be represented by multiple policies reflecting the complex nature of certain judicial branch entities. 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.

Priority and Baseline Allocation:

P1	LOW CM-1	MOD CM-1	HIGH CM-1

9.2 BASELINE CONFIGURATION

Control: The judicial branch entity develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

Recommendations: This control establishes baseline configurations for information systems and system components including communications and connectivity-related aspects of systems. Baseline configurations are documented, formally reviewed and agreed-upon sets of specifications for information systems or configuration items within those systems.

Baseline configurations serve as a basis for future builds, releases, and/or changes to information systems. Baseline configurations include information about information system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and patch information on operating systems and applications; and configuration settings/parameters), network topology, and the logical placement of those components within the system architecture. Maintaining baseline configurations requires creating new baselines as organizational information systems change over time. Baseline configurations of information systems reflect the current enterprise architecture.

Priority and Baseline Allocation:

P1	LOW CM-2	MOD CM-2 (1) (3) (7)	HIGH CM-2 (1) (2) (3) (7)

9.3 CONFIGURATION CHANGE CONTROL

Control: The judicial branch entity:

a. Determines the types of changes to the information system that are configuration-controlled;

b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;

c. Documents configuration change decisions associated with the information system;

d. Implements approved configuration-controlled changes to the information system;

e. Retains records of configuration-controlled changes to the information system for a five (5) year period;

f. Audits and reviews activities associated with configuration-controlled changes to the information system; and

g. Coordinates and provides oversight for configuration change control activities through on a monthly basis (or more frequently as required).

Recommendations: Configuration change controls for organizational information systems involve the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of information systems, changes to configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers, and mobile devices), unscheduled/unauthorized changes, and changes to remediate vulnerabilities. Typical processes for managing configuration changes to information

systems include, for example, Configuration Control Boards that approve proposed changes to systems. For new development information systems or systems undergoing major upgrades, judicial branch entities consider including representatives from development judicial branch entities on the Configuration Control Boards. Auditing of changes includes activities before and after changes are made to organizational information systems and the auditing activities required to implement such changes.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD CM-3 (2)	HIGH CM-3 (1) (2)

9.4 SECURITY IMPACT ANALYSIS

Control: The judicial branch entity analyzes changes to the information system to determine potential security impacts prior to change implementation.

Recommendations: 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 systems.

Priority and Baseline Allocation:

P2	LOW CM-4	MOD CM-4	HIGH CM-4 (1)

9.5 ACCESS RESTRICTIONS FOR CHANGE

Control: The judicial branch entity defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

Recommendations: 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, judicial branch entities permit only qualified and authorized individuals to access information systems for purposes of initiating changes, including upgrades and modifications. Judicial branch entities maintain records of access to ensure that configuration change control is implemented and to support after-the-fact actions should judicial branch entities discover any unauthorized changes. Access restrictions for change also include software libraries. Access restrictions include, for example, physical and logical

access controls, 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).

Priority and Baseline Allocation:

P1	**LOW Not Selected**	**MOD CM-5**	**HIGH CM-5 (1) (2) (3)**

9.6 CONFIGURATION SETTINGS

Control: The judicial branch entity:

a. Establishes and documents configuration settings for information technology products employed within the information system using industry standard security configuration checklists that reflect the most restrictive mode consistent with operational requirements;

b. Implements the configuration settings;

c. Identifies, documents, and approves any deviations from established configuration settings for defined information system components based on defined operational requirements; and

d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

Recommendations: 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. Judicial branch entities establish judicial branch entity-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 organizations in the public and private sectors. 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.

Priority and Baseline Allocation:

P1	LOW CM-6	MOD CM-6	HIGH CM-6 (1) (2)

9.7 LEAST FUNCTIONALITY

Control: The judicial branch entity:

a. Configures the information system to provide only essential capabilities; and

b. Prohibits or restricts the use of the following functions, ports, protocols, and/or services: [judicial branch entity-defined prohibited or restricted functions, ports, protocols, and/or services].

Recommendations: Information systems can provide a wide variety of functions and

services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from single information system components but doing so increases risk over limiting the services provided by any one component. Where feasible, judicial branch entities limit component functionality to a single function per device (e.g., email servers or web servers, but not both). Judicial branch entities review functions and services provided by information systems or individual components of information systems, to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, auto-execute, and file sharing). Judicial branch entities consider disabling unused or unnecessary physical and logical ports/protocols (e.g., Universal Serial Bus, File Transfer Protocol, and Hyper Text Transfer Protocol) on information systems to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling. Judicial branch entities can utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services.

Priority and Baseline Allocation:

P1	LOW CM-7	MOD CM-7 (1) (2) (4)	HIGH CM-7 (1) (2) (5)

9.8 INFORMATION SYSTEM COMPONENT INVENTORY

Control: The judicial branch entity:

a. Develops and documents an inventory of information system components that:

   1. Accurately reflects the current information system;

   2. Includes all components within the authorization boundary of the information system;

   3. Is at the level of granularity deemed necessary for tracking and reporting; and

   4. Includes [judicial branch entity defined information deemed necessary to achieve effective information system component accountability]; and

b. Reviews and updates the information system component on an annual basis.

Recommendations: Judicial branch entities may choose to implement centralized information system component inventories that include components from all organizational information systems. In such situations, judicial branch entities ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., information system association, information system owner). Information deemed necessary for effective accountability of information system components includes, for example, hardware inventory specifications, software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location.

Priority and Baseline Allocation:

P1	LOW CM-8	MOD CM-8 (1) (3) (5)	HIGH CM-8 (1) (2) (3) (4) (5)

9.9 CONFIGURATION MANAGEMENT PLAN

Control: The judicial branch entity 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 information system and places the configuration items under configuration management; and

d. Protects the configuration management plan from unauthorized disclosure and modification.

Recommendations: Configuration management plans satisfy the requirements in configuration management policies while being tailored to individual information systems. Such plans define detailed processes and procedures for how configuration management is used to support system development life cycle activities at the information system level. Configuration management plans are typically developed during the development/acquisition phase of the system development life cycle. The plans describe how to move changes through change management processes, how to update configuration settings and baselines, how to maintain information system component inventories, how to control development, test, and operational environments, and how to develop, release, and update key documents. Judicial branch entities can employ templates to help ensure consistent and timely development and implementation of configuration management plans. Such templates can represent a master configuration management plan for the judicial branch entity at large with subsets of the plan implemented on a system by system basis. Configuration management approval processes include designation of key management stakeholders responsible for reviewing and approving proposed changes to information systems, and personnel that conduct security impact analyses prior to the implementation of changes to the systems. Configuration items are the information system items (hardware, software, firmware, and documentation) to be configuration-managed. As information 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.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD CM-9	HIGH CM-9

9.10 SOFTWARE USAGE RESTRICTIONS

Control: The judicial branch entity:

a. Uses software and associated documentation in accordance with contract agreements and copyright laws;

b. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and

c. Controls and documents 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.

Recommendations: Software license tracking can be accomplished by manual methods (e.g., simple spreadsheets) or automated methods (e.g., specialized tracking applications) depending on organizational needs.

Priority and Baseline Allocation:

P2	LOW CM-10	MOD CM-10	HIGH CM-10

9.11 USER-INSTALLED SOFTWARE

Control: The judicial branch entity:

a. Establishes policies governing the installation of software by users;

b. Enforces software installation policies through judicial branch entity-defined methods; and

c. Monitors policy compliance on a semi-annual basis.

Recommendations: If provided the necessary privileges, users have the ability to install software in organizational information systems. To maintain control over the types of software installed, judicial branch entities identify permitted and prohibited actions regarding software installation. Permitted software installations may include, for example, updates and security patches to existing software and downloading applications from judicial branch entity-approved "app stores." Prohibited software installations may include, for example, software with unknown or suspect pedigrees or software that judicial branch entities consider potentially malicious. The policies judicial branch entities select governing user-installed software may be judicial branch entity-developed or provided by some external entity. Policy enforcement methods include procedural methods (e.g., periodic examination of user accounts), automated methods (e.g., configuration settings implemented on organizational information systems), or both.

Priority and Baseline Allocation:

P1	LOW CM-11	MOD CM-11	HIGH CM-11

10.0 CONTINGENCY PLANNING

10.1 CONTINGENCY PLANNING POLICY AND PROCEDURES

Control: The judicial branch entity:

a. Develops, documents, and disseminates to all workforce members:

   1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and

b. Reviews and updates the current:

   1. Contingency planning policy on an annual basis; and

   2. Contingency planning procedures on an annual basis.

Recommendations: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls in the CP family. Policy and procedures reflect applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the judicial branch entity 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 judicial branch entities or conversely, can be represented by multiple policies reflecting the complex nature of certain judicial branch entities. 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.

Priority and Baseline Allocation:

P1	LOW CP-1	MOD CP-1	HIGH CP-1

10.2 CONTINGENCY PLAN

Control: The judicial branch entity:

a. Develops a contingency plan for the information system that:

   1. Identifies essential missions 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 missions and business functions despite an information system disruption, compromise, or failure;

5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and

6. Is reviewed and approved by judicial branch entity-defined personnel or roles;

b. Distributes copies of the contingency plan to key contingency personnel and organizational elements;

c. Coordinates contingency planning activities with incident handling activities;

d. Reviews the contingency plan for the information system on an annual basis;

e. Updates the contingency plan to address changes to the judicial branch entity, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;

f. Communicates contingency plan changes to key contingency personnel and organizational elements; and

g. Protects the contingency plan from unauthorized disclosure and modification.

Recommendations: Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for mission/business functions. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. The effectiveness of contingency planning is maximized by considering such planning throughout the phases of the system development life cycle. Performing contingency planning on hardware, software, and firmware development can be an effective means of achieving information system resiliency. Contingency plans reflect the degree of restoration required for organizational information systems since not all systems may need to fully recover to achieve the level of continuity of operations desired. Information system recovery objectives reflect applicable laws, Executive Orders, directives, policies, standards, regulations, and guidelines. In addition to information system availability, contingency plans also address other security-related events resulting in a reduction in mission and/or business effectiveness, such as malicious attacks compromising the confidentiality or integrity of information systems. Actions addressed in contingency plans include, for example, orderly/graceful degradation, information system shutdown, fallback to a manual mode,

alternate information flows, and operating in modes reserved for when systems are under attack. By closely coordinating contingency planning with incident handling activities, judicial branch entities can ensure that the necessary contingency planning activities are in place and activated in the event of a security incident.

Priority and Baseline Allocation:

P1	**LOW CP-2**	**MOD CP-2 (1) (3) (8)**	**HIGH CP-2 (1) (2) (3) (4) (5) (8)**

10.3 CONTINGENCY TRAINING

Control: The judicial branch entity provides contingency training to information system users consistent with assigned roles and responsibilities:

a. Within six (6) months of assuming a contingency role or responsibility;

b. When required by information system changes; and

c. On an annual basis thereafter.

Recommendations: Contingency training provided by judicial branch entities 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, regular users 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 set up information systems at alternate processing and storage sites; and managers/senior leaders 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/responsibilities reflects the specific continuity requirements in the contingency plan.

Priority and Baseline Allocation:

P2	**LOW CP-3**	**MOD CP-3**	**HIGH CP-3 (1)**

10.4 CONTINGENCY PLAN TESTING

Control: The judicial branch entity:

a. Tests the contingency plan for the information system on an annual basis using defined tests to determine the effectiveness of the plan and the organizational readiness to execute the plan;

b. Reviews the contingency plan test results; and

c. Initiates corrective actions, if needed.

Recommendations: Methods for testing contingency plans to determine the effectiveness of the plans and to identify potential weaknesses in the plans include, for example, walk-through and tabletop exercises, checklists, simulations (parallel, full interrupt), and comprehensive exercises. Judicial branch entities conduct testing based on the continuity requirements in contingency plans and include a determination of the effects on organizational operations, assets, and individuals arising due to contingency operations. Judicial branch entities have flexibility and discretion in the breadth, depth, and timelines of corrective actions.

Priority and Baseline Allocation:

P2	**LOW CP-4**	**MOD CP-4 (1)**	**HIGH CP-4 (1) (2)**

10.5 ALTERNATE STORAGE SITE

Control: The judicial branch entity:

a. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and

b. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.

Recommendations: Alternate storage sites are sites that are geographically distinct from primary storage sites. An alternate storage site maintains duplicate copies of information and data in the event that the primary storage site is not available. Items covered by alternate storage site agreements include, for example, environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and coordination of delivery/retrieval of backup media. Alternate storage sites reflect the requirements in contingency plans so that judicial branch entities can maintain essential missions/business functions despite disruption, compromise, or failure in organizational information systems.

Priority and Baseline Allocation:

P1	**LOW Not Selected**	**MOD CP-6 (1) (3)**	**HIGH CP-6 (1) (2) (3)**

10.6 ALTERNATE PROCESSING SITE

Control: The judicial branch entity:

a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of judicial branch entity-defined information system operations for essential missions/business functions within a defined time period consistent with recovery time and recovery point objectives when the primary processing capabilities are unavailable;

b. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the judicial branch entity-defined time period for transfer/resumption; and

c. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.

Recommendations: 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.

Priority and Baseline Allocation:

P1	**LOW Not Selected**	**MOD CP-7 (1) (2) (3)**	**HIGH CP-7 (1) (2) (3)**

10.7 TELECOMMUNICATIONS SERVICES

Control: The judicial branch entity establishes alternate telecommunications services including necessary agreements to permit the resumption of judicial branch entity-defined information system operations for essential missions and business functions within a defined time period when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

Recommendations: This control applies to telecommunications services (data and voice) for primary and alternate processing and storage sites. Alternate telecommunications services reflect the continuity requirements in contingency plans to maintain essential missions/business functions despite the loss of primary telecommunications services. Judicial branch entities may specify different time periods for primary/alternate sites. Alternate telecommunications services include, for example, additional organizational or commercial ground-based circuits/lines or satellites in lieu of ground-based communications. Judicial branch entities consider factors such as availability, quality of service, and access when entering into alternate telecommunications agreements.

Priority and Baseline Allocation:

P1	**LOW Not Selected**	**MOD CP-8 (1) (2)**	**HIGH CP-8 (1) (2) (3) (4)**

10.8 INFORMATION SYSTEM BACKUP

Control: The judicial branch entity:

a. Conducts backups of user-level information contained in the information system on a judicial branch entity-defined frequency basis consistent with recovery time and recovery point objectives;

b. Conducts backups of system-level information contained in the information system on a judicial branch entity-defined frequency basis consistent with recovery time and recovery point objectives;

c. Conducts backups of information system documentation including security-related documentation on a judicial branch entity-defined frequency basis consistent with recovery time and recovery point objectives; and

d. Protects the confidentiality, integrity, and availability of backup information at storage locations.

Recommendations: System-level information includes, for example, system-state information, operating system and application software, and licenses. User-level information includes any information other than system-level information. Mechanisms employed by judicial branch entities to protect the integrity of information system backups include, for example, digital signatures and cryptographic hashes. Protection of system backup information while in transit is beyond the scope of this control. Information system backups reflect the requirements in contingency plans as well as other organizational requirements for backing up information.

Priority and Baseline Allocation:

P1	**LOW CP-9**	**MOD CP-9 (1)**	**HIGH CP-9 (1) (2) (3) (5)**

10.9 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION

Control: The judicial branch entity provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

Recommendations: Recovery is executing information system contingency plan activities to restore organizational missions/business functions. Reconstitution takes place following recovery and includes activities for returning organizational information systems to fully operational states. Recovery and reconstitution operations reflect mission and business priorities, recovery point/time and reconstitution objectives, and established organizational metrics consistent with contingency plan requirements. Reconstitution includes the deactivation of any interim information system capabilities that may have been needed during recovery operations. Reconstitution also includes assessments of fully restored information system capabilities, reestablishment of continuous monitoring activities, potential information system reauthorizations, and activities to prepare the systems against future disruptions, compromises, or failures. Recovery/reconstitution capabilities employed by judicial branch entities can include both automated mechanisms and manual procedures.

Priority and Baseline Allocation:

P1	**LOW CP-10**	**MOD CP-10 (2)**	**HIGH CP-10 (2) (4)**

11.0 IDENTIFICATION AND AUTHENTICATION

11.1 IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES

Control: The judicial branch entity:

a. Develops, documents, and disseminates to all workforce members:

   1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and

b. Reviews and updates the current:

   1. Identification and authentication policy on an annual basis; and

   2. Identification and authentication procedures on an annual basis.

Recommendations: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls in the IA family. Policy and procedures reflect applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the judicial branch entity 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 judicial branch entities or conversely, can be represented by multiple policies reflecting the complex nature of certain judicial branch entities. 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.

Priority and Baseline Allocation:

P1	LOW IA-1	MOD IA-1	HIGH IA-1

11.2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

Control: The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

Recommendations: Organizational users include employees or individuals that judicial branch entities deem to have equivalent status of employees (e.g., contractors, guest researchers). Judicial branch entities may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual

activity. Judicial branch entities employ passwords, tokens, or biometrics to authenticate user identities, or in the case multifactor authentication, or some combination thereof. Access to organizational information systems is defined as either local access or network access. Local access is any access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks (e.g., the Internet). Internal networks include local area networks and wide area networks. In addition, the use of encrypted virtual private networks (VPNs) for network connections between judicial branch entity-controlled endpoints and non-judicial branch entity-controlled endpoints may be treated as internal networks from the perspective of protecting the confidentiality and integrity of information traversing the network.

Multifactor authentication requires the use of two or more different factors to achieve authentication. The factors are defined as: (i) something you know (e.g., password, personal identification number (PIN)); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards. In addition to identifying and authenticating users at the information system level (i.e., at logon), judicial branch entities also employ identification and authentication mechanisms at the application level, when necessary, to provide increased information security.

Priority and Baseline Allocation:

P1	**LOW IA-2 (1) (12)**	**MOD IA-2 (1) (2) (3) (8) (11) (12)**	**HIGH IA-2 (1) (2) (3) (4) (8) (9) (11) (12)**

11.3 DEVICE IDENTIFICATION AND AUTHENTICATION

Control: The information system uniquely identifies and authenticates specifically defined and/or types of devices before establishing a local, network or remote connection.

Recommendations: 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. Judicial branch entities 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, judicial branch entities are encouraged to

only apply the control to those limited number (and type) of devices that truly need to support this capability.

Priority and Baseline Allocation:

P1	**LOW Not Selected**	**MOD IA-3**	**HIGH IA-3**

11.4 IDENTIFIER MANAGEMENT

Control: The judicial branch entity manages information system identifiers by:

a. Receiving authorization from judicial branch entity-defined personnel or roles to assign an individual, group, role, or device identifier;

b. Selecting an identifier that identifies an individual, group, role, or device;

c. Assigning the identifier to the intended individual, group, role, or device;

d. Preventing reuse of identifiers for a defined time period; and

e. Disabling the identifier after a defined time period of inactivity.

Recommendations: Common device identifiers include, for example, media access control (MAC), Internet protocol (IP) addresses, or device-unique token identifiers. Management of individual identifiers is not applicable to shared information system accounts (e.g., guest and anonymous accounts). This control also addresses individual identifiers not necessarily associated with information system accounts (e.g., identifiers used in physical security control databases accessed by badge reader systems for access to information systems). Preventing reuse of identifiers implies preventing the assignment of previously used individual, group, role, or device identifiers to different individuals, groups, roles, or devices.

Priority and Baseline Allocation:

P1	**LOW IA-4**	**MOD IA-4**	**HIGH IA-4**

11.5 AUTHENTICATOR MANAGEMENT

Control: The judicial branch entity manages information system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;

b. Establishing initial authenticator content for authenticators defined by the judicial branch entity;

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/compromised or damaged authenticators, and for revoking authenticators;

e. Changing default content of authenticators prior to information system installation;

f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;

g. Changing/refreshing authenticators on a judicial branch entity-defined time period by authenticator type basis;

h. Protecting authenticator content from unauthorized disclosure and modification;

i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and

j. Changing authenticators for group/role accounts when membership to those accounts changes.

Recommendations: Individual authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). In many cases, developers ship information system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security risk. Information systems support individual authenticator management by judicial branch entity-defined settings and restrictions for various authenticator characteristics including, for example, minimum password length, password composition, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication. Specific actions that can be taken to safeguard authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing individual authenticators with others, and reporting lost, stolen, or compromised authenticators immediately. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include, for example, certificates and passwords.

Priority and Baseline Allocation:

P1	LOW IA-5 (1) (11)	MOD IA-5 (1) (2) (3) (11)	HIGH IA-5 (1) (2) (3) (11)

11.6 AUTHENTICATOR FEEDBACK

Control: The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Recommendations: The feedback from information systems does not provide information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of information systems or system components, for example, desktops/notebooks with relatively large monitors, the threat (often referred to as shoulder surfing) may be significant. For other types of systems or components, for example, mobile devices with 2 to 4-inch screens, this threat may be less significant, and may need to be balanced against the increased likelihood of typographic input errors due to the small keyboards. Therefore, the means for obscuring the authenticator feedback is selected accordingly. Obscuring the feedback of authentication information includes, for example, displaying asterisks when users type passwords into input devices, or displaying feedback for a very limited time before fully obscuring it.

Priority and Baseline Allocation:

P2	LOW IA-6	MOD IA-6	HIGH IA-6

11.7 CRYPTOGRAPHIC MODULE AUTHENTICATION

Control: The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal and state laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

Recommendations: 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.

Priority and Baseline Allocation:

P1	LOW IA-7	MOD IA-7	HIGH IA-7

11.8 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)

Control: The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

Recommendations: Authentication of non-organizational users accessing judicial branch entity information systems may be required to protect judicial branch entity, State, proprietary, or privacy-related information (with exceptions noted for national security systems). Judicial branch entities use risk assessments to determine authentication needs and consider scalability, practicality, and security in balancing the need to ensure ease of use for

access to federal information and information systems with the need to protect and adequately mitigate risk.

Priority and Baseline Allocation:

P1	**LOW IA-8 (1) (2) (3) (4)**	**MOD IA-8 (1) (2) (3) (4)**	**HIGH IA-8 (1) (2) (3) (4)**

12.0 INCIDENT RESPONSE

12.1 INCIDENT RESPONSE POLICY AND PROCEDURES

Control: The judicial branch entity:

a. Develops, documents, and disseminates to all workforce members:

   1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and

b. Reviews and updates the current:

   1. Incident response policy on an annual basis; and

   2. Incident response procedures on an annual basis.

Recommendations: This requirement set addresses the establishment of policy and procedures for the effective implementation of selected security controls in the IR family. Policy and procedures reflect applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the judicial branch entity 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 judicial branch entities or conversely, can be represented by multiple policies reflecting the complex nature of certain judicial branch entities. 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.

Priority and Baseline Allocation:

P1	LOW IR-1	MOD IR-1	HIGH IR-1

12.2 INCIDENT RESPONSE TRAINING

Control: The judicial branch entity provides incident response training to information system users consistent with assigned roles and responsibilities:

a. Within six (6) months of assuming an incident response role or responsibility;

b. When required by information system changes; and

c. Every two (2) years thereafter.

Recommendations: Incident response training provided by judicial branch entities is linked to the assigned roles and responsibilities of organizational personnel to ensure the appropriate content and level of detail is included in such training. For example, regular users may only need to know who to call or how to recognize an incident on the information system; system administrators may require additional training on how to handle/remediate incidents; and incident responders may receive more specific training on forensics, reporting, system recovery, and restoration. Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources.

Priority and Baseline Allocation:

P2	**LOW IR-2**	**MOD IR-2**	**HIGH IR-2 (1) (2)**

12.3 INCIDENT RESPONSE TESTING

Control: The judicial branch entity tests the incident response capability for the information system on an annual basis using defined tests to determine the incident response effectiveness and documents the results.

Recommendations: Judicial branch entities test incident response capabilities to determine the overall effectiveness of the capabilities and to identify potential weaknesses or deficiencies. Incident response testing includes, for example, the use of checklists, walk-through or tabletop exercises, simulations (parallel/full interrupt), and comprehensive exercises. Incident response testing can also include a determination of the effects on organizational operations (e.g., reduction in mission capabilities), organizational assets, and individuals due to incident response.

Priority and Baseline Allocation:

P2	**LOW Not Selected**	**MOD IR-3 (2)**	**HIGH IR-3 (2)**

12.4 INCIDENT HANDLING

Control: The judicial branch entity:

a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;

b. Coordinates incident handling activities with contingency planning activities; and

c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

Recommendations: Judicial branch entities recognize that incident response capability is dependent on the capabilities of organizational information systems and the mission/business processes being supported by those systems. Therefore, judicial branch entities consider incident response as part of the definition, design, and development of mission/business processes and information systems. Incident-related information can be obtained from a variety of sources including, for example, audit monitoring, network monitoring, physical access monitoring, user/administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities including, for example, mission/business owners, information system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive (function).

Priority and Baseline Allocation:

P1	LOW IR-4	MOD IR-4 (1)	HIGH IR-4 (1) (4)

12.5 INCIDENT MONITORING

Control: The judicial branch entity tracks and documents information system security incidents.

Recommendations: Documenting information system security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

Priority and Baseline Allocation:

P1	LOW IR-5	MOD IR-5	HIGH IR-5 (1)

12.6 INCIDENT REPORTING

Control: The judicial branch entity:

a. Requires workforce members to report suspected security incidents to the judicial branch entity incident response capability immediately upon discovery; and

b. Reports security incident information to the judicial branch entity-defined personnel or roles responsible for the incident response process.

Recommendations: The intent of this control is to address both specific incident reporting requirements within a judicial branch entity and the formal incident reporting requirements for State agencies. 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 and state laws, Executive Orders, directives, regulations, policies, standards, and guidance.

Priority and Baseline Allocation:

P1	LOW IR-6	MOD IR-6 (1)	HIGH IR-6 (1)

12.7 INCIDENT RESPONSE ASSISTANCE

Control: The judicial branch entity 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.

Recommendations: Incident response support resources provided by judicial branch entities include, for example, help desks, assistance groups, and access to forensics services, when required.

Priority and Baseline Allocation:

P2	LOW IR-7	MOD IR-7 (1)	HIGH IR-7 (1)

12.8 INCIDENT RESPONSE PLAN

Control: The judicial branch entity:

a. Develops an incident response plan that:

   1. Provides the judicial branch entity with a roadmap for implementing its incident response capability;

   2. Describes the structure and judicial branch entity 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 judicial branch entity, which relate to mission, size, structure, and functions;

   5. Defines reportable incidents;

   6. Provides metrics for measuring the incident response capability within the judicial branch entity;

   7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and

8. Is reviewed and approved by judicial branch entity-defined personnel or roles.;

b. Distributes copies of the incident response plan to the incident response personnel and business unit owners;

c. Reviews the incident response plan on an annual basis;

d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;

e. Communicates incident response plan changes to the incident response personnel and business unit owners; and

f. Protects the incident response plan from unauthorized disclosure and modification.

Recommendations: It is important that judicial branch entities develop and implement a coordinated approach to incident response. Organizational missions, business functions, strategies, goals, and objectives for incident response help to determine the structure of incident response capabilities. As part of a comprehensive incident response capability, judicial branch entities consider the coordination and sharing of information with other judicial branch entities (as appropriate) and external organizations, including, for example, external service providers and organizations involved in the supply chain for organizational information systems.

Priority and Baseline Allocation:

P1	LOW IR-8	MOD IR-8	HIGH IR-8

13.0 MAINTENANCE

13.1 SYSTEM MAINTENANCE POLICY AND PROCEDURES

Control: The judicial branch entity:

a. Develops, documents, and disseminates to all workforce members:

   1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and

b. Reviews and updates the current:

   1. System maintenance policy on an annual basis; and

   2. System maintenance procedures on an [entity-defined frequency] basis.

Recommendations: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls in the MA family. Policy and procedures reflect applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the judicial branch entity 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 judicial branch entities or conversely, can be represented by multiple policies reflecting the complex nature of certain judicial branch entities. 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.

Priority and Baseline Allocation:

P1	LOW MA-1	MOD MA-1	HIGH MA-1

13.2 CONTROLLED MAINTENANCE

Control: The judicial branch entity:

a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;

b. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;

c. Requires that the CIO or designee explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;

d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;

e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and

f. Includes judicial branch entity-defined maintenance-related information in organizational maintenance records.

Recommendations: This control addresses the information security aspects of the information system maintenance program and applies to all types of maintenance to any system component (including applications) conducted by any local or nonlocal entity (e.g., in-contract, warranty, in-house, software maintenance agreement). System maintenance also includes those components not directly associated with information processing and/or data/information retention such as scanners, copiers, and printers. Information necessary for creating effective maintenance records includes, for example: (i) date and time of maintenance; (ii) name of individuals or group performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) information system components/equipment removed or replaced (including identification numbers, if applicable). The level of detail included in maintenance records can be informed by the security categories of organizational information systems. Judicial branch entities consider supply chain issues associated with replacement components for information systems.

Priority and Baseline Allocation:

P2	LOW MA-2	MOD MA-2	HIGH MA-2 (2)

13.3 MAINTENANCE TOOLS

Control: The judicial branch entity approves, controls, and monitors information system maintenance tools.

Recommendations: This control addresses security-related issues associated with maintenance tools used specifically for diagnostic and repair actions on organizational information systems. Maintenance tools can include hardware, software, and firmware items. Maintenance tools are potential vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and subsequently into organizational information systems. Maintenance tools can include, for example, hardware/software

diagnostic test equipment and hardware/software packet sniffers. This control does not cover hardware/software components that may support information system maintenance, yet are a part of the system, for example, the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch.

Priority and Baseline Allocation:

P3	LOW Not Selected	MOD MA-3 (1) (2)	HIGH MA-3 (1) (2) (3)

13.4 NON-LOCAL MAINTENANCE

Control: The judicial branch entity:

a. Approves and monitors nonlocal maintenance and diagnostic activities;

b. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;

c. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;

d. Maintains records for nonlocal maintenance and diagnostic activities; and

e. Terminates session and network connections when nonlocal maintenance is completed.

Recommendations: Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection. Typically, strong authentication requires authenticators that are resistant to replay attacks and employ multifactor authentication. Strong authenticators include, for example, PKI where certificates are stored on a token protected by a password, passphrase, or biometric. Enforcing requirements is accomplished in part by other controls.

Priority and Baseline Allocation:

P2	LOW MA-4	MOD MA-4 (2)	HIGH MA-4 (2) (3)

13.5 MAINTENANCE PERSONNEL

Control: The judicial branch entity:

a. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;

b. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and

c. Designates judicial branch entity personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

Recommendations: This control applies to individuals performing hardware or software maintenance on organizational information systems. Technical competence of supervising individuals relates to the maintenance performed on the information 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 information systems, for example, when required to conduct maintenance activities with little or no notice. Based on organizational assessments of risk, judicial branch entities may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for very limited time periods.

Priority and Baseline Allocation:

P2	LOW MA-5	MOD MA-5	HIGH MA-5 (1)

13.6 TIMELY MAINTENANCE

Control: The judicial branch entity obtains maintenance support and/or spare parts for judicial branch entity-defined information system components within a judicial branch entity-defined time period of failure.

Recommendations: Judicial branch entities specify the information system components that result in increased risk to organizational operations and assets, individuals, other organizations, or the State when the functionality provided by those components is not operational. Organizational actions to obtain maintenance support typically include having appropriate contracts in place.

Priority and Baseline Allocation:

P2	LOW Not Selected	MOD MA-6	HIGH MA-6

14.0 MEDIA PROTECTION

14.1 MEDIA PROTECTION POLICY AND PROCEDURES

Control: The judicial branch entity:

a. Develops, documents, and disseminates to all workforce members:

   1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and

b. Reviews and updates the current:

   1. Media protection policy on an annual basis; and

   2. Media protection procedures on an annual basis.

Recommendations: This requirement set addresses the establishment of policy and procedures for the effective implementation of selected security controls in the MP family. Policy and procedures reflect applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the judicial branch entity 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 judicial branch entities or conversely, can be represented by multiple policies reflecting the complex nature of certain judicial branch entities. 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.

Priority and Baseline Allocation:

P1	LOW MP-1	MOD MP-1	HIGH MP-1

14.2 MEDIA ACCESS

Control: The judicial branch entity restricts access to judicial branch entity-defined types of digital and/or non-digital media to judicial branch entity-defined personnel or roles.

Recommendations: Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Restricting non-digital media access includes, for example,

denying access to patient medical records in a community hospital unless the individuals seeking access to such records are authorized healthcare providers. Restricting access to digital media includes, for example, limiting access to design specifications stored on compact disks in the media library to the project leader and the individuals on the development team.

Priority and Baseline Allocation:

P2	LOW MP-2	MOD MP-2	HIGH MP-2

14.3 MEDIA MARKING

Control: The judicial branch entity:

a. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and

b. Exempts judicial branch entity-defined types of information system media from marking as long as the media remain within controlled areas.

Recommendations: The term security marking refers to the application/use of human-readable security attributes. The term security labeling refers to the application/use of security attributes with regard to internal data structures within information systems. Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Security marking is generally not required for media containing information determined by judicial branch entities to be in the public domain or to be publicly releasable. However, some judicial branch entities may require markings for public information indicating that the information is publicly releasable. Marking of information system media reflects applicable federal and state laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD MP-3	HIGH MP-3

14.4 MEDIA STORAGE

Control: The judicial branch entity:

a. Physically controls and securely stores judicial branch entity-defined types of digital and/or non-digital media within judicial branch entity-defined controlled areas; and

b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Recommendations: Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Physically controlling information system media includes, for example, conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the media library, and maintaining accountability for all stored media. Secure storage includes, for example, a locked drawer, desk, or cabinet, or a controlled media library. The type of media storage is commensurate with the security category and/or classification of the information residing on the media. Controlled areas are areas for which judicial branch entities provide sufficient physical and procedural safeguards to meet the requirements established for protecting information and/or information systems. For media containing information determined by judicial branch entities to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on judicial branch entities or individuals if accessed by other than authorized personnel, fewer safeguards may be needed. In these situations, physical access controls provide adequate protection.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD MP-4	HIGH MP-4

14.5 MEDIA TRANSPORT

Control: The judicial branch entity:

a. Protects and controls judicial branch entity-defined types of information system media during transport outside of controlled areas using judicial branch entity-defined security safeguards;

b. Maintains accountability for information system media during transport outside of controlled areas;

c. Documents activities associated with the transport of information system media; and

d. Restricts the activities associated with the transport of information system media to authorized personnel.

Recommendations: Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. This control also applies to mobile devices with information storage capability (e.g., smart phones, tablets, E-readers), that are transported outside of controlled areas. Controlled areas are areas or spaces for which judicial branch entities provide sufficient physical and/or procedural safeguards to meet the requirements established for protecting information and/or information systems.

Physical and technical safeguards for media are commensurate with the security category or classification of the information residing on the media. Safeguards to protect media during transport include, for example, locked containers and cryptography. Cryptographic mechanisms can provide confidentiality and integrity protections depending upon the mechanisms used. Activities associated with transport include the actual transport as well as those activities such as releasing media for transport and ensuring that media enters the appropriate transport processes. For the actual transport, authorized transport and courier personnel may include individuals from outside the judicial branch entity (e.g., U.S. Postal Service or a commercial transport or delivery service). Maintaining accountability of media during transport includes, for example, restricting transport activities to authorized personnel, and tracking and/or obtaining explicit records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering. Judicial branch entities establish documentation requirements for activities associated with the transport of information system media in accordance with organizational assessments of risk to include the flexibility to define different record-keeping methods for the different types of media transport as part of an overall system of transport-related records.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD MP-5 (4)	HIGH MP-5 (4)

14.6 MEDIA SANITIZATION

Control: The judicial branch entity:

a. Sanitizes judicial branch entity-defined information system media prior to disposal, release out of organizational control, or release for reuse using judicial branch entity-defined sanitization techniques and procedures in accordance with applicable organizational standards and policies; and

b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

Recommendations: This control applies to all information system media, both digital and non-digital, subject to disposal or reuse, whether or not the media is considered removable. Examples include media found in scanners, copiers, printers, notebook computers, workstations, network components, and mobile devices. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Judicial branch entities determine the appropriate sanitization methods recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization. Judicial branch entities use discretion on the employment of approved sanitization techniques and procedures for media containing

information deemed to be in the public domain or publicly releasable or deemed to have no adverse impact on judicial branch entities or individuals if released for reuse or disposal. Sanitization of non-digital media includes, for example, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections/words in a manner equivalent in effectiveness to removing them from the document.

Priority and Baseline Allocation:

P1	LOW MP-6	MOD MP-6	HIGH MP-6 (1) (2) (3)

14.7 MEDIA USE

Control: The judicial branch entity restricts or prohibits the use of judicial branch entity-defined types of information system media on judicial branch entity-defined information systems or system components using judicial branch entity-defined security safeguards.

Recommendations: Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. This control also applies to mobile devices with information storage capability (e.g., smart phones, tablets, E-readers). In contrast to Media Access, which restricts user access to media, this control restricts the use of certain types of media on information systems, for example, restricting/prohibiting the use of flash drives or external hard disk drives. Judicial branch entities can employ technical and nontechnical safeguards (e.g., policies, procedures, rules of behavior) to restrict the use of information system media. Judicial branch entities 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/removing the ability to insert, read or write to such devices. Judicial branch entities may also limit the use of portable storage devices to only approved devices including, for example, devices provided by the judicial branch entity, devices provided by other approved organizations, and devices that are not personally owned. Finally, judicial branch entities may restrict the use of portable storage devices based on the type of device, for example, prohibiting the use of writeable, portable storage devices, and implementing this restriction by disabling or removing the capability to write to such devices.

Priority and Baseline Allocation:

P1	LOW MP-7	MOD MP-7 (1)	HIGH MP-7 (1)

15.0 PHYSICAL AND ENVIRONMENTAL PROTECTION

15.1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES

Control: The judicial branch entity:

a. Develops, documents, and disseminates to all workforce members:

   1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and

b. Reviews and updates the current:

   1. Physical and environmental protection policy on an annual basis; and

   2. Physical and environmental protection procedures on an annual basis.

Recommendations: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls in the PE family. Policy and procedures reflect applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the judicial branch entity 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 judicial branch entities or conversely, can be represented by multiple policies reflecting the complex nature of certain judicial branch entities. 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.

Priority and Baseline Allocation:

P1	LOW PE-1	MOD PE-1	HIGH PE-1

15.2 PHYSICAL ACCESS AUTHORIZATIONS

Control: The judicial branch entity:

a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;

b. Issues authorization credentials for facility access;

c. Reviews the access list detailing authorized facility access by individuals on a monthly basis; and

d. Removes individuals from the facility access list when access is no longer required.

Recommendations: This control applies to judicial branch entity workforce members and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Authorization credentials include, for example, badges, identification cards, and smart cards. Judicial branch entities determine the strength of authorization credentials needed (including level of forge-proof badges, smart cards, or identification cards) consistent with judicial branch entity standards, policies, and procedures. This control only applies to areas within facilities that have not been designated as publicly accessible.

Priority and Baseline Allocation:

P1	LOW PE-2	MOD PE-2	HIGH PE-2

15.3 PHYSICAL ACCESS CONTROL

Control: The judicial branch entity:

a. Enforces physical access authorizations at judicial branch entity-defined entry/exit points to the facility where the information system resides by;

1. Verifying individual access authorizations before granting access to the facility; and

2. Controlling ingress/egress to the facility using judicial branch entity-defined physical access control systems/devices and/or guards;

b. Maintains physical access audit logs for judicial branch entity-defined entry/exit points;

c. Provides judicial branch entity-defined security safeguards to control access to areas within the facility officially designated as publicly accessible;

d. Escorts visitors and monitors visitor activity for judicial branch entity-defined circumstances requiring visitor escorts and monitoring;

e. Secures keys, combinations, and other physical access devices;

f. Inventories of judicial branch entity-defined physical access devices on a judicial branch entity-defined frequency; and

g. Changes combinations and keys on a judicial branch entity-defined frequency and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

Recommendations: This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Judicial branch entities determine the types of facility guards needed including, for example, professional physical security staff or other personnel such as administrative staff or information system users. Physical access devices include, for example, keys, locks, combinations, and card readers. Safeguards for publicly accessible areas within organizational facilities include, for example, cameras, monitoring by guards, and isolating selected information systems and/or system components in secured areas. Physical access control systems comply with applicable federal and state laws, Executive Orders, directives, policies, regulations, standards, and guidance. Judicial branch entities have flexibility in the types of audit logs employed. Audit logs can be procedural (e.g., a written log of individuals accessing the facility and when such access occurred), automated (e.g., capturing ID provided by a PIV card), or some combination thereof. Physical access points can include facility access points, interior access points to information systems and/or components requiring supplemental access controls, or both. Components of organizational information systems (e.g., workstations, terminals) may be located in areas designated as publicly accessible with judicial branch entities safeguarding access to such devices.

Priority and Baseline Allocation:

P1	**LOW PE-3**	**MOD PE-3**	**HIGH PE-3 (1)**

15.4 ACCESS CONTROL FOR TRANSMISSION MEDIUM

Control: The judicial branch entity controls physical access to defined information system distribution and transmission lines within organizational facilities using judicial branch entity-defined security safeguards.

Recommendations: Physical security safeguards applied to information system distribution and transmission lines help to prevent accidental damage, disruption, and physical tampering. In addition, physical safeguards may be necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Security safeguards to control physical access to system distribution and transmission lines include, for example: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays.

Priority and Baseline Allocation:

P1	**LOW Not Selected**	**MOD PE-4**	**HIGH PE-4**

15.5 ACCESS CONTROL FOR OUTPUT DEVICES

Control: The judicial branch entity controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

Recommendations: Controlling physical access to output devices includes, for example, placing output devices in locked rooms or other secured areas and allowing access to authorized individuals only, and placing output devices in locations that can be monitored by organizational personnel. Monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of information system output devices.

Priority and Baseline Allocation:

P2	LOW Not Selected	MOD PE-5	HIGH PE-5

15.6 MONITORING PHYSICAL ACCESS

Control: The judicial branch entity:

a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;

b. Reviews physical access logs on judicial branch entity-defined frequency basis and upon occurrence of judicial branch entity-defined events or potential indications of events; and

c. Coordinates results of reviews and investigations with the organizational incident response capability.

Recommendations: Judicial branch entities incident response capabilities include investigations of and responses to detected physical security incidents. Security incidents include, for example, apparent security violations or suspicious physical access activities. Suspicious physical access activities include, for example: (i) accesses outside of normal work hours; (ii) repeated accesses to areas not normally accessed; (iii) accesses for unusual lengths of time; and (iv) out-of-sequence accesses.

Priority and Baseline Allocation:

P1	LOW PE-6	MOD PE-6 (1)	HIGH PE-6 (1) (4)

15.7 VISITOR ACCESS RECORDS

Control: The judicial branch entity:

a. Maintains visitor access records to the facility where the information system resides for a judicial branch entity-defined time period; and

b. Reviews visitor access records on a monthly basis.

Recommendations: Visitor access records include, for example, names and organization of persons visiting, visitor signatures, forms of identification, dates of access, entry and departure times, purposes of visits, and names of persons visited. Visitor access records are not required for publicly accessible areas.

Priority and Baseline Allocation:

P3	**LOW PE-8**	**MOD PE-8**	**HIGH PE-8 (1)**

15.8 POWER EQUIPMENT AND CABLING

Control: The judicial branch entity protects power equipment and power cabling for the information system from damage and destruction.

Recommendations: Judicial branch entities determine the types of protection necessary for power equipment and cabling employed at different locations both internal and external to organizational facilities and environments of operation. This includes, for example, generators and power cabling outside of buildings, internal cabling and uninterruptable power sources within an office or data center, and power sources for self-contained entities such as vehicles and satellites.

Priority and Baseline Allocation:

P1	**LOW Not Selected**	**MOD PE-9**	**HIGH PE-9**

15.9 EMERGENCY SHUTOFF

Control: The judicial branch entity:

a. Provides the capability of shutting off power to the information system or individual system components in emergency situations;

b. Places emergency shutoff switches or devices in judicial branch entity-defined location by information system or system component to facilitate safe and easy access for personnel; and

c. Protects emergency power shutoff capability from unauthorized activation.

Recommendations: This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms.

Priority and Baseline Allocation:

P1	**LOW Not Selected**	**MOD PE-10**	**HIGH PE-10**

15.10 EMERGENCY POWER

Control: The judicial branch entity provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system and/or transition of the information system to long-term alternate power in the event of a primary power source loss.

Recommendations: Reference Contingency Plan and Alternate Processing Site above.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD PE-11	HIGH PE-11 (1)

15.11 EMERGENCY LIGHTING

Control: The judicial branch entity employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

Recommendations: This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms.

Priority and Baseline Allocation:

P1	LOW PE-12	MOD PE-12	HIGH PE-12

15.12 FIRE PROTECTION

Control: The judicial branch entity employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

Recommendations: This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.

Priority and Baseline Allocation:

P1	LOW PE-13	MOD PE-13 (3)	HIGH PE-13 (1) (2) (3)

15.13 TEMPERATURE AND HUMIDITY CONTROLS

Control: The judicial branch entity:

a. Maintains temperature and humidity levels within the facility where the information system resides at judicial branch entity-defined acceptable levels; and

b. Monitors temperature and humidity levels on a judicial branch entity-defined frequency basis.

Recommendations: This control applies primarily to facilities containing concentrations of information system resources, for example, data centers, server rooms, and mainframe computer rooms.

Priority and Baseline Allocation:

P1	LOW PE-14	MOD PE-14	HIGH PE-14

15.14 WATER DAMAGE PROTECTION

Control: The judicial branch entity protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

Recommendations: This control applies primarily to facilities containing concentrations of information system resources including, for example, 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 judicial branch entities.

Priority and Baseline Allocation:

P1	LOW PE-15	MOD PE-15	HIGH PE-15 (1)

15.15 DELIVERY AND REMOVAL

Control: The judicial branch entity authorizes, monitors, and controls defined types of information system components entering and exiting the facility and maintains records of those items.

Recommendations: Effectively enforcing authorizations for entry and exit of information system components may require restricting access to delivery areas and possibly isolating the areas from the information system and media libraries.

Priority and Baseline Allocation:

P2	LOW PE-16	MOD PE-16	HIGH PE-16

15.16 ALTERNATE WORK SITE

Control: The judicial branch entity:

a. Employs judicial branch entity-defined security controls at alternate work sites;

b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and

c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

Recommendations: Alternate work sites may include, for example, government facilities or private residences of employees. While commonly distinct from alternative processing sites, alternate work sites may provide readily available alternate locations as part of contingency

operations. Judicial branch entities may define different sets of security controls for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites. This control supports the contingency planning activities of judicial branch entities and the applicable telework initiatives.

Priority and Baseline Allocation:

P2	LOW Not Selected	MOD PE-17	HIGH PE-17

15.17 LOCATION OF INFORMATION SYSTEM COMPONENTS

Control: The judicial branch entity positions information system components within the facility to minimize potential damage from defined physical and environmental hazards and to minimize the opportunity for unauthorized access.

Recommendations: Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation. In addition, judicial branch entities consider the location of physical entry points where unauthorized individuals, while not being granted access, might nonetheless be in close proximity to information systems and therefore increase the potential for unauthorized access to organizational communications (e.g., through the use of wireless sniffers or microphones).

Priority and Baseline Allocation:

P3	LOW Not Selected	MOD Not Selected	HIGH PE-18

16.0 PLANNING

16.1 SECURITY PLANNING POLICY AND PROCEDURES

Control: The judicial branch entity:

a. Develops, documents, and disseminates to workforce members:

   1. A security planning 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 planning policy and associated security planning controls; and

b. Reviews and updates the current:

   1. Security planning policy on an annual basis; and

   2. Security planning procedures on an annual basis.

Recommendations: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls in the PL family. Policy and procedures reflect applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the judicial branch entity 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 judicial branch entities or conversely, can be represented by multiple policies reflecting the complex nature of certain judicial branch entities. 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.

Priority and Baseline Allocation:

P1	LOW PL-1	MOD PL-1	HIGH PL-1

16.2 SYSTEM SECURITY PLAN

Control: The judicial branch entity:

a. Develops a security plan for the information system that:

   1. Is consistent with the judicial branch entity's enterprise architecture;

   2. Explicitly defines the authorization boundary for the system;

3. Describes the operational context of the information system in terms of missions and business processes;

4. Provides the security categorization of the information system including supporting rationale;

5. Describes the operational environment for the information system and relationships with or connections to other information systems;

6. Provides an overview of the security requirements for the system;

7. Identifies any relevant overlays, if applicable;

8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and

9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;

b. Distributes copies of the security plan and communicates subsequent changes to the plan to the judicial branch entity-defined personnel or roles;

c. Reviews the security plan for the information system on an annual basis and after significant changes;

d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and

e. Protects the security plan from unauthorized disclosure and modification.

Recommendations: Security plans relate security requirements to a set of security controls. Security plans also describe, at a high level, how the security controls 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 judicial branch entities, and the State if the plan is implemented as intended. Judicial branch entities can also apply tailoring guidance to the security control baselines in Appendix D in NIST SP 800-53 to develop overlays for community-wide use or to address specialized requirements, technologies, or missions/environments of operation Appendix I in NIST SP 800-53 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.

Priority and Baseline Allocation:

P1	LOW PL-2	MOD PL-2 (3)	HIGH PL-2 (3)

16.3 RULES OF BEHAVIOR

Control: The judicial branch entity:

a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage;

b. Receives a signed 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 information system;

c. Reviews and updates the rules of behavior on an annual basis; and

d. Requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated.

Recommendations: This control enhancement applies to organizational users. Judicial branch entities consider rules of behavior based on individual user roles and responsibilities, differentiating, for example, 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, for example, individuals who simply receive data/information from federal information systems, is often not feasible given the large number of such users and the limited nature of their interactions with the systems.

Priority and Baseline Allocation:

P2	LOW PL-4	MOD PL-4 (1)	HIGH PL-4 (1)

16.4 INFORMATION SECURITY ARCHITECTURE

Control: The judicial branch entity:

a. Develops an information security architecture for the information system that:

    1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;

    2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and

    3. Describes any information security assumptions about, and dependencies on, external services;

b. Reviews and updates the information security architecture on an annual basis to reflect updates in the enterprise architecture; and

c. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS) (as described by NIST control PL-7 in NIST 800-53, and organizational procurements/acquisitions.

Recommendations: This control addresses actions taken by judicial branch entities 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, judicial branch entity-wide information security architecture 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 judicial branch entities 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 CSO to ensure that security controls needed to support privacy requirements are identified and effectively implemented. This control is primarily directed at judicial branch entities (i.e., internally focused) to help ensure that judicial branch entities 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 judicial branch entity-wide information security architecture.

Priority and Baseline Allocation:

P1	**LOW Not Selected**	**MOD PL-8**	**HIGH PL-8**

17.0 PERSONNEL SECURITY

17.1 PERSONNEL SECURITY POLICY AND PROCEDURES

Control: The judicial branch entity:

a. Develops, documents, and disseminates to the organization:

   1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and

b. Reviews and updates the current:

   1. Personnel security policy on an annual basis; and

   2. Personnel security procedures on an annual basis.

Recommendations: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls in the PS family. Policy and procedures reflect applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the judicial branch entity 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 judicial branch entities or conversely, can be represented by multiple policies reflecting the complex nature of certain judicial branch entities. 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.

Priority and Baseline Allocation:

P1	LOW PS-1	MOD PS-1	HIGH PS-1

17.2 POSITION RISK DESIGNATION

Control: The judicial branch entity:

a. Assigns a risk designation to all organizational positions;

b. Establishes screening criteria for individuals filling those positions; and

c. Reviews and updates position risk designations on an annual basis.

Recommendations: Position risk designations reflect Human Resources policy and guidance. Risk designations can guide and inform the types of authorizations individuals receive when accessing organizational information and information systems. Position screening criteria include explicit information security role appointment requirements (e.g., training, security clearances).

Priority and Baseline Allocation:

P1	LOW PS-2	MOD PS-2	HIGH PS-2

17.3 PERSONNEL SCREENING

Control: The judicial branch entity:

a. Screens individuals prior to authorizing access to the information system; and

b. Rescreens individuals according to Human Resources policy.

Recommendations: Personnel screening and rescreening activities reflect applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, guidance, and specific criteria established for the risk designations of assigned positions. Judicial branch entities may define different rescreening conditions and frequencies for personnel accessing information systems based on types of information processed, stored, or transmitted by the systems.

Priority and Baseline Allocation:

P1	LOW PS-3	MOD PS-3	HIGH PS-3

17.4 PERSONNEL TERMINATION

Control: The judicial branch entity, upon termination of individual employment:

a. Disables information system access immediately/within 24 hours;

b. Terminates/revokes any authenticators/credentials associated with the individual;

c. Conducts exit interviews that include a discussion of judicial branch entity-defined information security topics;

d. Retrieves all security-related organizational information system-related property;

e. Retains access to organizational information and information systems formerly controlled by terminated individual; and

f. Notifies judicial branch entity-defined personnel or roles within judicial branch entity-defined time period.

Recommendations: Information system-related property includes, for example, 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 information system-related property. Security topics of interest at exit interviews can include, for example, reminding terminated individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not be possible for some terminated individuals, for example, in cases related to job abandonment, illnesses, and non-availability of supervisors. Exit interviews are important for individuals with security clearances. Timely execution of termination actions is essential for individuals terminated for cause. In certain situations, judicial branch entities consider disabling the information system accounts of individuals that are being terminated prior to the individuals being notified.

Priority and Baseline Allocation:

P1	LOW PS-4	MOD PS-4	HIGH PS-4 (2)

17.5 PERSONNEL TRANSFER

Control: The judicial branch entity:

a. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the judicial branch entity;

b. Initiates judicial branch entity-defined transfer or reassignment actions within judicial branch entity-defined time period following the formal transfer action;

c. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and

d. Notifies judicial branch entity-defined personnel or roles within judicial branch entity-defined time period.

Recommendations: This control applies when reassignments or transfers of individuals are permanent or of such extended durations as to make the actions warranted. Judicial branch entities 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 judicial branch entities include, for example: (i) returning old and issuing new keys, identification cards, and building passes; (ii) closing information system accounts and establishing new accounts; (iii) changing information system access authorizations (i.e., privileges); and (iv) providing for access to official records to which individuals had access at previous work locations and in previous information system accounts.

Priority and Baseline Allocation:

P2	LOW PS-5	MOD PS-5	HIGH PS-5

17.6 ACCESS AGREEMENTS

Control: The judicial branch entity:

a. Develops and documents access agreements for organizational information systems;

b. Reviews and updates the access agreements on an annual basis; and

c. Ensures that individuals requiring access to organizational information and information systems:

   1. Sign appropriate access agreements prior to being granted access; and

   2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or on an annual basis.

Recommendations: Access agreements include, for example, 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 information systems to which access is authorized. Judicial branch entities can use electronic signatures to acknowledge access agreements unless specifically prohibited by organizational policy.

Priority and Baseline Allocation:

P3	LOW PS-6	MOD PS-6	HIGH PS-6

17.7 THIRD-PARTY PERSONNEL SECURITY

Control: The judicial branch entity:

a. Establishes personnel security requirements including security roles and responsibilities for third-party providers;

b. Requires third-party providers to comply with personnel security policies and procedures established by the judicial branch entity;

c. Documents personnel security requirements;

d. Requires third-party providers to notify judicial branch entity-defined personnel or roles of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within judicial branch entity-defined time period; and

e. Monitors provider compliance.

Recommendations: Third-party providers include, for example, service bureaus, contractors, and other judicial branch entities providing information system development, information technology services, outsourced applications, and network and security management. Judicial branch entities explicitly include personnel security requirements in acquisition-related documents. Third-party providers may have personnel working at organizational facilities with credentials, badges, or information system privileges issued by judicial branch entities. Notifications of third-party personnel changes ensure appropriate termination of privileges and credentials. Judicial branch entities define the transfers and terminations deemed reportable by security-related characteristics that include, for example, functions, roles, and nature of credentials/privileges associated with individuals transferred or terminated.

Priority and Baseline Allocation:

P1	LOW PS-7	MOD PS-7	HIGH PS-7

17.8 PERSONNEL SANCTIONS

Control: The judicial branch entity:

a. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and

b. Notifies judicial branch entity-defined personnel or roles within four (4) hours when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

Recommendations: Organizational sanctions processes reflect applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, and guidance. Sanctions processes are described in access agreements and can be included as part of general personnel policies and procedures for judicial branch entities. Judicial branch entities consult with the Office of the General Counsel regarding matters of employee sanctions.

Priority and Baseline Allocation:

P3	LOW PS-8	MODPS-8	HIGH PS-8

18.0 RISK ASSESSMENT

18.1 RISK ASSESSMENT POLICY AND PROCEDURES

Control: The judicial branch entity:

a. Develops, documents, and disseminates to all workforce members:

   1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and

b. Reviews and updates the current:

   1. Risk assessment policy on an annual basis; and

   2. Risk assessment procedures on an annual basis.

Recommendations: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls in the RA family. Policy and procedures reflect applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the judicial branch entity 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 judicial branch entities or conversely, can be represented by multiple policies reflecting the complex nature of certain judicial branch entities. 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.

Priority and Baseline Allocation:

P1	LOW RA-1	MOD RA-1	HIGH RA-1

18.2 SECURITY CATEGORIZATION

Control: The judicial branch entity:

a. Categorizes information and the information system in accordance with applicable federal and state laws, Executive Orders, directives, policies, regulations, standards, and guidance;

b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and

c. Ensures that the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.

Recommendations: Clearly defined authorization boundaries are a prerequisite for effective security categorization decisions. Security categories describe the potential adverse impacts to organizational operations, organizational assets, and individuals if organizational information and information systems are comprised through a loss of confidentiality, integrity, or availability. Judicial branch entities conduct the security categorization process as a judicial branch entity-wide activity with the involvement of chief information officers, senior information security officers, information system owners, mission/business owners, and information owners/stewards. Judicial branch entities also consider the potential adverse impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level adverse impacts. Security categorization processes carried out by judicial branch entities facilitate the development of inventories of information assets, mappings to specific information system components where information is processed, stored, or transmitted.

Priority and Baseline Allocation:

P1	LOW RA-2	MOD RA-2	HIGH RA-2

18.3 RISK ASSESSMENT

Control: The judicial branch entity:

a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;

b. Documents risk assessment results in a risk assessment report;

c. Reviews risk assessment results on an annual basis;

d. Disseminates risk assessment results to judicial branch entity-defined personnel or roles; and

e. Updates the risk assessment on an annual basis or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

Recommendations: Clearly defined authorization boundaries are a prerequisite for effective risk assessments. Risk assessments take into account threats, vulnerabilities, likelihood, and

impact to organizational operations and assets, individuals, other judicial branch entities, and the State based on the operation and use of information systems. Risk assessments also take into account risk from external parties (e.g., service providers, contractors operating information systems on behalf of the judicial branch entity, individuals accessing organizational information systems, outsourcing entities).

Risk assessments (either formal or informal) can be conducted at all three tiers in the risk management hierarchy (i.e., judicial branch entity level, mission/business process level, or information system level) and at any phase in the system development life cycle. Risk assessments can also be conducted at various steps in the Risk Management Framework, including categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring. Risk assessments can play an important role in security control selection processes, particularly during the application of tailoring guidance, which includes security control supplementation.

Priority and Baseline Allocation:

P1	LOW RA-3	MOD RA-3	HIGH RA-3

18.4 VULNERABILITY SCANNING

Control: The judicial branch entity:

a. Scans for vulnerabilities in the information system and hosted applications on a quarterly basis and/or randomly in accordance with entity-defined process and when new vulnerabilities potentially affecting the system/applications are identified and reported;

b. Employs vulnerability scanning 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;

c. Analyzes vulnerability scan reports and results from security control assessments;

d. Remediates legitimate vulnerabilities in a judicial branch entity-defined response times in accordance with an organizational assessment of risk; and

e. Shares information obtained from the vulnerability scanning process and security control assessments with judicial branch entity-defined personnel or roles to help eliminate

similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

Recommendations: Security categorization of information systems guides the frequency and comprehensiveness of vulnerability scans. Judicial branch entities 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. Judicial branch entities 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. Judicial branch entities 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. Judicial branch entities also consider using tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS).

Priority and Baseline Allocation:

P1	**LOW RA-5**	**MOD RA-5 (1) (2) (5)**	**HIGH RA-5 (1) (2) (4) (5)**

19.0 SYSTEM AND SERVICES ACQUISITION

19.1 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES

Control: The judicial branch entity:

a. Develops, documents, and disseminates to the organization:

   1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and

b. Reviews and updates the current:

   1. System and services acquisition policy on an annual basis; and

   2. System and services acquisition procedures on an annual basis.

Recommendations: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls in the SA family. Policy and procedures reflect applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the judicial branch entity 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 judicial branch entities or conversely, can be represented by multiple policies reflecting the complex nature of certain judicial branch entities. 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.

Priority and Baseline Allocation:

P1	LOW SA-1	MOD SA-1	HIGH SA-1

19.2 ALLOCATION OF RESOURCES

Control: The judicial branch entity:

a. Determines information security requirements for the information system or information system service in mission/business process planning;

b. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and

c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.

Recommendations: Resource allocation for information security includes funding for the initial information system or information system service acquisition and funding for the sustainment of the system/service.

Priority and Baseline Allocation:

P1	LOW SA-2	MOD SA-2	HIGH SA-2

19.3 SYSTEM DEVELOPMENT LIFE CYCLE

Control: The judicial branch entity:

a. Manages the information system using a judicial branch entity-defined system development life cycle that incorporates information security considerations;

b. Defines and documents information security roles and responsibilities throughout the system development life cycle;

c. Identifies individuals having information security roles and responsibilities; and

d. Integrates the organizational information security risk management process into system development life cycle activities.

Recommendations: A well-defined system development life cycle provides the foundation for the successful development, implementation, and operation of organizational information systems. To apply the required security controls within the system development life cycle requires a basic understanding of information security, threats, vulnerabilities, adverse impacts, and risk to critical missions/business functions. The security engineering principles cannot be properly applied if individuals that design, code, and test information systems and system components (including information technology products) do not understand security. Therefore, judicial branch entities include qualified personnel, for example, chief information security officers, security architects, security engineers, and information system security officers in system development life cycle activities to ensure that security requirements are incorporated into organizational information systems. It is equally important that developers include individuals on the development team that possess the requisite security expertise and skills to ensure that needed security capabilities are effectively integrated into the information system. Security awareness and training programs can help ensure that individuals having key security roles and responsibilities have the

appropriate experience, skills, and expertise to conduct assigned system development life cycle activities. The effective integration of security requirements into enterprise architecture also helps to ensure that important security considerations are addressed early in the system development life cycle and that those considerations are directly related to the organizational mission/business processes. This process also facilitates the integration of the information security architecture into the enterprise architecture, consistent with organizational risk management and information security strategies.

Priority and Baseline Allocation:

P1	LOW SA-3	MOD SA-3	HIGH SA-3

19.4 ACQUISITION PROCESS

Control: The judicial branch entity includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal and state laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

a. Security functional requirements;

b. Security strength requirements;

c. Security assurance requirements;

d. Security-related documentation requirements;

e. Requirements for protecting security-related documentation;

f. Description of the information system development environment and environment in which the system is intended to operate; and

g. Acceptance criteria.

Recommendations: Information system components are discrete, identifiable information technology assets (e.g., hardware, software, or firmware) that represent the building blocks of an information system. Information system components include commercial information technology products. Security functional requirements include security capabilities, security functions, and security mechanisms. Security strength requirements associated with such capabilities, functions, and mechanisms include degree of correctness, completeness, resistance to direct attack, and resistance to tampering or bypass. Security assurance requirements include: (i) development processes, procedures, practices, and methodologies; and (ii) evidence from development and assessment activities providing grounds for confidence that the required security functionality has been implemented and the required

security strength has been achieved. Security documentation requirements address all phases of the system development life cycle.

Security functionality, assurance, and documentation requirements are expressed in terms of security controls that have been selected through the tailoring process. The security control tailoring process includes, for example, the specification of parameter values through the use of assignment and selection statements and the specification of platform dependencies and implementation information. Security documentation provides user and administrator guidance regarding the implementation and operation of security controls. The level of detail required in security documentation is based on the security category or classification level of the information system and the degree to which judicial branch entities depend on the stated security capability, functions, or mechanisms to meet overall risk response expectations (as defined in the organizational risk management strategy). Security requirements can also include organizationally mandated configuration settings specifying allowed functions, ports, protocols, and services. Acceptance criteria for information systems, information system components, and information system services are defined in the same manner as such criteria for any organizational acquisition or procurement.

Priority and Baseline Allocation:

P1	LOW SA-4 (10)	MOD SA-4 (1) (2) (9) (10)	HIGH SA-4 (1) (2) (9) (10)

19.5 INFORMATION SYSTEM DOCUMENTATION

Control: The judicial branch entity:

a. Obtains administrator documentation for the information system, system component, or information system service that describes:

   1. Secure configuration, installation, and operation of the system, component, or service;

   2. Effective use and maintenance of security functions/mechanisms; and

   3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;

b. Obtains user documentation for the information system, system component, or information system service that describes:

   1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;

   2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and

3. User responsibilities in maintaining the security of the system, component, or service;

c. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and takes judicial branch entity-defined actions in response;

d. Protects documentation as required, in accordance with the risk management strategy; and

e. Distributes documentation to judicial branch entity-defined personnel or roles.

Recommendations: This control helps organizational personnel understand the implementation and operation of security controls associated with information systems, system components, and information system services. Judicial branch entities consider establishing specific measures to determine the quality/completeness of the content provided. The inability to obtain needed documentation may occur, for example, due to the age of the information system/component or lack of support from developers and contractors. In those situations, judicial branch entities may need to recreate selected documentation if such documentation is essential to the effective implementation or operation of security controls. The level of protection provided for selected information system, component, or service documentation is commensurate with the security category or classification of the system. Documentation that addresses information system vulnerabilities may also require an increased level of protection. Secure operation of the information system, includes, for example, initially starting the system and resuming secure system operation after any lapse in system operations.

Priority and Baseline Allocation:

P2	LOW SA-5	MOD SA-5	HIGH SA-5

19.6 SECURITY ENGINEERING PRINCIPLES

Control: The judicial branch entity applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

Recommendations: Judicial branch entities apply security engineering principles primarily to new development information systems or systems undergoing major upgrades. For legacy systems, judicial branch entities apply security engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware within those systems. Security engineering principles include, for example: (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design; (iii) incorporating security requirements into the system development life cycle; (iv) delineating physical and logical security boundaries; (v)

ensuring that system developers are trained on how to build secure software; (vi) tailoring security controls to meet organizational and operational needs; (vii) performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and (viii) reducing risk to acceptable levels, thus enabling informed risk management decisions.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD SA-8	HIGH SA-8

19.7 EXTERNAL INFORMATION SYSTEM SERVICES

Control: The judicial branch entity:

a. Requires that providers of external information system services comply with organizational information security requirements and employ judicial branch entity-defined security controls in accordance with applicable federal and state laws, Executive Orders, directives, policies, regulations, standards, and guidance;

b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and

c. Employs judicial branch entity-defined processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis.

Recommendations: External information system services are services that are implemented outside of the authorization boundaries of organizational information systems. This includes services that are used by, but not a part of, organizational information systems. Judicial branch entities establish relationships with external service providers in a variety of ways including, for example, through joint ventures, business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, and supply chain exchanges. The responsibility for managing risks from the use of external information system services remains with authorizing officials. For services external to judicial branch entities, a chain of trust requires that judicial branch entities establish and retain a level of confidence that each participating provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered. The extent and nature of this chain of trust varies based on the relationships between judicial branch entities and the external providers. Judicial branch entities document the basis for trust relationships so the relationships can be monitored over time. External information system services documentation includes government, service providers, end user security roles and responsibilities, and service-level agreements. Service-level agreements define expectations of performance for security controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance.

Priority and Baseline Allocation:

P1	LOW SA-9	MOD SA-9 (2)	HIGH SA-9 (2)

19.8 DEVELOPER CONFIGURATION MANAGEMENT

Control: The judicial branch entity 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, and operation as applicable;

b. Document, manage, and control the integrity of changes to judicial branch entity-defined configuration items under configuration management;

c. Implement only judicial branch entity-approved changes to the system, component, or service;

d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and

e. Track security flaws and flaw resolution within the system, component, or service and report findings to judicial branch entity-defined personnel.

Recommendations: This requirement set also applies to judicial branch entities conducting internal information systems development and integration. Judicial branch entities consider the quality and completeness of the configuration management activities conducted by developers as evidence of applying effective security safeguards. Safeguards include, for example, protecting from unauthorized modification or destruction, the master copies of all material used to generate security-relevant portions of the system hardware, software, and firmware. Maintaining the integrity of changes to the information system, information system component, or information system service requires configuration control throughout the system development life cycle to track authorized changes and prevent unauthorized changes. Configuration items that are placed under configuration management (if existence/use is required by other security controls) include: the formal model; the functional, high-level, and low-level design specifications; other design data; implementation documentation; source code and hardware schematics; the running version of the object code; tools for comparing new versions of security-relevant hardware descriptions and software/firmware source code with previous versions; and test fixtures and documentation. Depending on the mission/business needs of judicial branch entities and the nature of the contractual relationships in place, developers may provide configuration management support during the operations and maintenance phases of the life cycle.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD SA-10	HIGH SA-10

19.9 DEVELOPER SECURITY TESTING AND EVALUATION

Control: The judicial branch entity requires the developer of the information system, system component, or information system service to:

a. Create and implement a security assessment plan;

b. Perform unit, integration, system, regression testing/evaluation at a judicial branch entity-defined depth and coverage;

c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;

d. Implement a verifiable flaw remediation process; and

e. Correct flaws identified during security testing/evaluation.

Recommendations: 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.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD SA-11	HIGH SA-11

19.10 SUPPLY CHAIN PROTECTION

Control: The judicial branch entity protects against supply chain threats to the information system, system component, or information system service by employing judicial branch entity-defined security safeguards as part of a comprehensive, defense-in-breadth information security strategy.

Recommendations: Information systems (including system components that compose those systems) need to be protected throughout the system development life cycle (i.e., during design, development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and retirement). Protection of organizational information systems is accomplished through threat awareness, by the identification, management, and reduction of vulnerabilities at each phase of the life cycle and the use of complementary, mutually reinforcing strategies to respond to risk. Judicial branch entities consider implementing a standardized process to address supply chain risk with respect to information systems and system components, and to educate the acquisition workforce on threats, risk, and required security controls. Judicial branch entities use the acquisition/procurement processes to require supply chain entities to implement necessary security safeguards to: (i) reduce the likelihood of unauthorized modifications at each stage in the supply chain; and (ii) protect information systems and information system components, prior to taking delivery of such systems/components. This control enhancement also applies to information system services. Security safeguards include, for example: (i) security controls for development systems, development facilities, and external connections to development systems; (ii) vetting development personnel; and (iii) use of tamper-evident packaging during shipping/warehousing. Methods for reviewing and protecting development plans, evidence, and documentation are commensurate with the security category or classification level of the information system. Contracts may specify documentation protection requirements.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD Not Selected	HIGH SA-12

19.11 DEVELOPMENT PROCESS, STANDARDS, AND TOOLS

Control: The judicial branch entity:

a. Requires the developer of the information system, system component, or information system service to follow a documented development process that:

   1. Explicitly addresses security 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. Reviews the development process, standards, tools, and tool options/configurations on a judicial branch entity-defined frequency basis to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy judicial branch entity-defined security requirements.

Recommendations: Development tools include, for example, programming languages and computer-aided design (CAD) systems. Reviews of development processes can include, for example, the use of maturity models to determine the potential effectiveness of such processes. Maintaining the integrity of changes to tools and processes enables accurate supply chain risk assessment and mitigation, and requires robust configuration control throughout the life cycle (including design, development, transport, delivery, integration, and maintenance) to track authorized changes and prevent unauthorized changes.

Priority and Baseline Allocation:

P2	LOW Not Selected	MOD Not Selected	HIGH SA-15

19.12 DEVELOPER-PROVIDED TRAINING

Control: The judicial branch entity requires the developer of the information system, system component, or information system service to provide judicial branch entity-defined training on the correct use and operation of the implemented security functions, controls, and/or mechanisms.

Recommendations: This control applies to external and internal (in-house) developers. Training of personnel is an essential element to ensure the effectiveness of security controls implemented within organizational information systems. Training options include, for example, classroom-style training, web-based/computer-based training, and hands-on training. Judicial branch entities can also request sufficient training materials from developers to conduct in-house training or offer self-training to organizational personnel. Judicial branch entities determine the type of training necessary and may require different types of training for different security functions, controls, or mechanisms.

Priority and Baseline Allocation:

P2	LOW Not Selected	MOD Not Selected	HIGH SA-16

19.13 DEVELOPER SECURITY ARCHITECTURE AND DESIGN

Control: The judicial branch entity requires the developer of the information system, system component, or information system service to produce a design specification and security architecture that:

a. Is consistent with and supportive of the judicial branch entity's security architecture which is established within and is an integrated part of the judicial branch entity's enterprise architecture;

b. Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and

c. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.

Recommendations: This control is primarily directed at external developers, although it could also be used for internal (in-house) development.

Priority and Baseline Allocation:

P1	**LOW Not Selected**	**MOD Not Selected**	**HIGH SA-17**

20.0 SYSTEM AND COMMUNICATIONS PROTECTION

20.1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES

Control: The judicial branch entity:

a. Develops, documents, and disseminates to all workforce members:

   1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and

b. Reviews and updates the current:

   1. System and communications protection policy on an annual basis; and

   2. System and communications protection procedures on an annual basis.

Recommendations: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls in the SC family. Policy and procedures reflect applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the judicial branch entity 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 judicial branch entities or conversely, can be represented by multiple policies reflecting the complex nature of certain judicial branch entities. 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.

Priority and Baseline Allocation:

P1	LOW SC-1	MOD SC-1	HIGH SC-1

20.2 APPLICATION PARTITIONING

Control: The information system separates user functionality (including user interface services) from information system management functionality.

Recommendations: 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. Judicial branch

entities 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.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD SC-2	HIGH SC-2

20.3 SECURITY FUNCTION ISOLATION

Control: The information system isolates security functions from non-security functions.

Recommendations: 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.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD Not Selected	HIGH SC-3

20.4 INFORMATION IN SHARED RESOURCES

Control: The information system prevents unauthorized and unintended information transfer via shared system resources.

Recommendations: This requirement set prevents information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems. The control of information in shared resources is also commonly

referred to as object reuse and residual information protection. This control does not address: (i) information remanence which refers to residual representation of data that has been nominally erased or removed; (ii) covert channels (including storage and/or timing channels) where shared resources are manipulated to violate information flow restrictions; or (iii) components within information systems for which there are only single users/roles.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD SC-4	HIGH SC-4

20.5 DENIAL OF SERVICE PROTECTION

Control: The information system protects against or limits the effects of judicial branch entity-defined types of denial of service attacks: by employing judicial branch entity-defined security safeguards.

Recommendations: A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect information system components on internal organizational networks from being directly affected by denial of service attacks. Employing increased capacity and bandwidth combined with service redundancy may also reduce the susceptibility to denial of service attacks.

Priority and Baseline Allocation:

P1	LOW SC-5	MOD SC-5	HIGH SC-5

20.6 BOUNDARY PROTECTION

Control: The information system:

a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;

b. Implements sub-networks for publicly accessible system components that are physically or logically separated from internal organizational networks; and

c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

Recommendations: Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a security architecture (e.g., routers protecting firewalls or application gateways residing on protected sub-networks). Sub-networks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces within organizational information systems

includes, for example, restricting external web traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses. Judicial branch entities consider the shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers and may also include third party-provided access lines and other service elements. Such transmission services may represent sources of increased risk despite contract security provisions.

Priority and Baseline Allocation:

P1	**LOW SC-7**	**MOD SC-7 (3) (4) (5) (7)**	**HIGH SC-7 (3) (4) (5) (7) (8) (18) (21)**

20.7 TRANSMISSION CONFIDENTIALITY AND INTEGRITY

Control: The information system protects the confidentiality and integrity of transmitted information.

Recommendations: This requirement set applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification. Protecting the confidentiality and/or integrity of organizational information can be accomplished by physical means (e.g., by employing protected distribution systems) or by logical means (e.g., employing encryption techniques). Judicial branch entities relying on commercial providers offering transmission services as commodity services rather than as fully dedicated services (i.e., services which can be highly specialized to individual customer needs), may find it difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality/integrity. In such situations, judicial branch entities determine what types of confidentiality/integrity services are available in standard, commercial telecommunication service packages. If it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, judicial branch entities implement appropriate compensating security controls or explicitly accept the additional risk.

Priority and Baseline Allocation:

P1	**LOW Not Selected**	**MOD SC-8 (1)**	**HIGH SC-8 (1)**

20.8 NETWORK DISCONNECT

Control: The information system terminates the network connection associated with a communications session at the end of the session or after judicial branch entity-defined time period of inactivity.

Recommendations: This control applies to both internal and external networks. Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection. Time periods of inactivity may be established by judicial branch entities and include, for example, time periods by type of network access or for specific network accesses.

Priority and Baseline Allocation:

P2	LOW Not Selected	MOD SC-10	HIGH SC-10

20.9 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Control: The judicial branch entity establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with judicial branch entity-defined requirements for key generation, distribution, storage, access, and destruction.

Recommendations: Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. Judicial branch entities define key management requirements in accordance with applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, and guidance, specifying appropriate options, levels, and parameters. Judicial branch entities manage trust stores to ensure that only approved trust anchors are in such trust stores. This includes certificates with visibility external to organizational information systems and certificates related to the internal operations of systems.

Priority and Baseline Allocation:

P1	LOW SC-12	MOD SC-12	HIGH SC-12 (1)

20.10 CRYPTOGRAPHIC PROTECTION

Control: The information system implements cryptographic methods based on judicial branch entity-defined requirements in accordance with applicable federal and state laws, Executive Orders, directives, policies, regulations, and standards.

Recommendations: Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified and Controlled Unclassified Information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the

necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. This control does not impose any requirements on judicial branch entities to use cryptography. However, if cryptography is required based on the selection of other security controls, judicial branch entities define each type of cryptographic use and the type of cryptography required (e.g., protection of classified information: NSA-approved cryptography; provision of digital signatures: FIPS-validated cryptography).

Priority and Baseline Allocation:

P1	LOW SC-13	MOD SC-13	HIGH SC-13

20.11 COLLABORATIVE COMPUTING DEVICES

Control: The information system:

a. Prohibits remote activation of collaborative computing devices except where defined exceptions are allowed; and

b. Provides an explicit indication of use to users physically present at the devices.

Recommendations: Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated.

Priority and Baseline Allocation:

P1	LOW SC-15	MOD SC-15	HIGH SC-15

20.12 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

Control: The judicial branch entity issues public key certificates under a judicial branch entity-defined certificate policy or obtains public key certificates from an approved service provider.

Recommendations: For all certificates, judicial branch entities manage information system trust stores to ensure only approved trust anchors are in the trust stores. This control addresses both certificates with visibility external to organizational information systems and certificates related to the internal operations of systems, for example, application-specific time services.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD SC-17	HIGH SC-17

20.13 MOBILE CODE

Control: The judicial branch entity:

a. Defines acceptable and unacceptable mobile code and mobile code technologies;

b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and

c. Authorizes, monitors, and controls the use of mobile code within the information system.

Recommendations: Decisions regarding the employment of mobile code within organizational information systems are based on the potential for the code to cause damage to the systems if used maliciously. Mobile code technologies include, for example, Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices (e.g., smart phones). Mobile code policy and procedures address preventing the development, acquisition, or introduction of unacceptable mobile code within organizational information systems.

Priority and Baseline Allocation:

P2	LOW Not Selected	MOD SC-18	HIGH SC-18

20.14 VOICE OVER INTERNET PROTOCOL

Control: The judicial branch entity:

a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and

b. Authorizes, monitors, and controls the use of VoIP within the information system.

Recommendations: None

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD SC-19	HIGH SC-19

20.15 SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

Control: The information system:

a. Provides 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. Provides 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.

Recommendations: This control enables external clients including, for example, 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. Information systems that provide name and address resolution services include, for example, domain name system (DNS) servers. Additional artifacts include, for example, DNS Security (DNSSEC) digital signatures and cryptographic keys. DNS resource records are examples of authoritative data. The means to indicate the security status of child zones includes, for example, the use of delegation signer resource records in the DNS. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to assure the authenticity and integrity of response data.

Priority and Baseline Allocation:

P1	LOW SC-20	MOD SC-20	HIGH SC-20

20.16 SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)

Control: 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.

Recommendations: 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.

Priority and Baseline Allocation:

P1	LOW SC-21	MOD SC-21	HIGH SC-21

20.17 ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE

Control: The information systems that collectively provide name/address resolution service for a judicial branch entity are fault-tolerant and implement internal/external role separation.

Recommendations: Information systems that provide name and address resolution services include, for example, domain name system (DNS) servers. To eliminate single points of failure and to enhance redundancy, judicial branch entities employ at least two authoritative domain name system servers, one configured as the primary server and the other configured as the secondary server. Additionally, judicial branch entities typically deploy the servers in two geographically separated network sub-networks (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 judicial branch entities (i.e., from internal clients). DNS servers with external roles only process name and address resolution information requests from clients external to judicial branch entities (i.e., on external networks including the Internet). Judicial branch entities specify clients that can access authoritative DNS servers in particular roles (e.g., by address ranges, explicit lists).

Priority and Baseline Allocation:

P1	LOW SC-22	MOD SC-22	HIGH SC-22

20.18 SESSION AUTHENTICITY

Control: The information system protects the authenticity of communications sessions.

Recommendations: This control addresses communications protection at the session, versus packet level (e.g., sessions in service-oriented architectures providing web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted. Authenticity protection includes, for example, protecting against man-in-the-middle attacks/session hijacking and the insertion of false information into sessions.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD SC-23	HIGH SC-23

20.19 FAIL IN KNOWN STATE

Policy: The information system fails to a known-state for judicial branch entity-defined types of failures preserving judicial branch entity-defined system state information in failure.

Recommendations: Failure in a known state addresses security concerns in accordance with the mission/business needs of judicial branch entities. 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 judicial branch entities with less disruption of mission/business processes.

Priority and Baseline Allocation:

P1	**LOW Not Selected**	**MOD Not Selected**	**HIGH SC-24**

20.20 PROTECTION OF INFORMATION AT REST

Control: The information system protects the confidentiality and integrity of judicial branch entity-defined information at rest.

Recommendations: This control addresses the confidentiality and integrity of information at rest and covers user information and system information. Information at rest refers to the state of information when it is located on storage devices as specific components of information systems. System-related information requiring protection includes, for example, configurations or rule sets for firewalls, gateways, intrusion detection/prevention systems, filtering routers, and authenticator content. Judicial branch entities 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. Judicial branch entities may also employ other security controls including, for example, secure off-line storage in lieu of online storage when adequate protection of information at rest cannot otherwise be achieved and/or continuous monitoring to identify malicious code at rest.

Priority and Baseline Allocation:

P1	**LOW Not Selected**	**MOD SC-28**	**HIGH SC-28**

20.21 PROCESS ISOLATION

Control: The information system maintains a separate execution domain for each executing process.

Recommendations: Information systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each information 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. This capability is available in most commercial operating systems that employ multi-state processor technologies.

Priority and Baseline Allocation:

P1	**LOW SC-39**	**MOD SC-39**	**HIGH SC-39**

21.0 SYSTEM AND INFORMATION INTEGRITY

21.1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES

Control: The judicial branch entity:

a. Develops, documents, and disseminates to all workforce members:

   1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and

b. Reviews and updates the current:

   1. System and information integrity policy on an annual basis; and

   2. System and information integrity procedures on an annual basis.

Recommendations: This requirement set addresses the establishment of policy and procedures for the effective implementation of selected security controls in the SI family. Policy and procedures reflect applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the judicial branch entity 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 judicial branch entities or conversely, can be represented by multiple policies reflecting the complex nature of certain judicial branch entities. 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.

Priority and Baseline Allocation:

P1	LOW SI-1	MOD SI-1	HIGH SI-1

21.2 FLAW REMEDIATION

Control: The judicial branch entity:

a. Identifies, reports, and corrects information system flaws;

b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

c. Installs security-relevant software and firmware updates within a judicial branch entity-defined time period of the release of the updates; and

d. Incorporates flaw remediation into the organizational configuration management process.

Recommendations: Judicial branch entities identify information systems affected by announced software flaws including potential vulnerabilities resulting from those flaws and report this information to designated organizational personnel with information security responsibilities. Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures. Judicial branch entities also address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Judicial branch entities take advantage of available resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems. By incorporating flaw remediation into ongoing configuration management processes, required/anticipated remediation actions can be tracked and verified. Flaw remediation actions that can be tracked and verified include, for example, determining whether judicial branch entities follow US-CERT guidance and Information Assurance Vulnerability Alerts. Judicial branch entity-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including, for example, the security category of the information system or the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types. Judicial branch entities determine the degree and type of testing needed for the specific type of flaw remediation activity under consideration and also the types of changes that are to be configuration-managed. In some situations, judicial branch entities may determine that the testing of software and/or firmware updates is not necessary or practical, for example, when implementing simple anti-virus signature updates. Judicial branch entities may also consider in testing decisions, whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures.

Priority and Baseline Allocation:

P1	LOW SI-2	MOD SI-2 (2)	HIGH SI-2 (1) (2)

21.3 MALICIOUS CODE PROTECTION

Control: The judicial branch entity:

a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;

b. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;

c. Configures malicious code protection mechanisms to:

   1. Perform periodic scans of the information system daily and real-time scans of files from external sources at endpoints and/or network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy; and

   2. Block or quarantine malicious code, and send alert to administrator, or take other judicial branch entity-defined action(s) as appropriate in response to malicious code detection; and

d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

Recommendations: Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using steganography. Malicious code can be transported by different means including, for example, web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of information system vulnerabilities. Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber-attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, judicial branch entities rely instead on other safeguards including, for example, secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Judicial branch entities may determine that in response to the detection of malicious code, different actions may be warranted. For example, judicial branch entities can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads, and/or actions in response to detection of maliciousness when attempting to open or execute files.

Priority and Baseline Allocation:

P1	LOW SI-3	MOD SI-3 (1) (2)	HIGH SI-3 (1) (2)

21.4 INFORMATION SYSTEM MONITORING

Control: The judicial branch entity:

a. Monitors the information system to detect:

   1. Attacks and indicators of potential attacks in accordance with judicial branch entity-defined monitoring objectives; and

   2. Unauthorized local, network, and remote connections;

b. Identifies unauthorized use of the information system through judicial branch entity-defined techniques and methods;

c. Deploys monitoring devices:

   1. Strategically within the information system to collect judicial branch entity-determined essential information; and

   2. at ad hoc locations within the system to track specific types of transactions of interest to the judicial branch entity;

d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;

e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, including other judicial branch entities, or the State based on law enforcement information, intelligence information, or other credible sources of information;

f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal and state laws, Executive Orders, directives, policies, or regulations; and

g. Provides judicial branch entity-defined information system monitoring information to judicial branch entity-defined personnel or roles on an as needed basis.

Recommendations: Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the information system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the information system. Judicial branch entities can monitor information systems, for example, 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 may guide

determination of the events. Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include, for example, selected perimeter locations and near server farms supporting critical applications, with such devices typically being employed at managed interfaces associated with controls defined in Boundary Protection and Remote Access above. The granularity of monitoring information collected is based on organizational monitoring objectives and the capability of information systems to support such objectives. Specific types of transactions of interest include, for example, Hyper Text Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. Information system monitoring is an integral part of organizational continuous monitoring and incident response programs. Output from system monitoring serves as input to continuous monitoring and incident response programs. A network connection is any connection with a device that communicates through a network (e.g., local area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Local, network, and remote connections can be either wired or wireless.

Priority and Baseline Allocation:

P1	LOW SI-4	MOD SI-4 (2) (4) (5)	HIGH SI-4 (2) (4) (5)

21.5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

Control: The judicial branch entity:

a. Receives information system security alerts, advisories, and directives from judicial branch entity-defined external organizations on an ongoing basis;

b. Generates internal security alerts, advisories, and directives as deemed necessary;

c. Disseminates security alerts, advisories, and directives to designated personnel, roles and/or entities both internal and external to the judicial branch entity as appropriate; and

d. Implements security directives in accordance with established time frames or notifies the issuing judicial branch entity of the degree of noncompliance.

Recommendations: The United States Computer Emergency Readiness Team (US-CERT) generates security alerts and advisories to maintain situational awareness across the federal government. Compliance to 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 judicial branch entities, and the State should the directives not be implemented in a timely manner. External judicial branch entities include, for example, external mission/business partners, supply chain partners, external service providers, and other peer/supporting judicial branch entities.

Priority and Baseline Allocation:

P1	LOW SI-5	MOD SI-5	HIGH SI-5 (1)

21.6 SECURITY FUNCTION VERIFICATION

Control: The information system:

a. Verifies the correct operation of judicial branch entity-defined security functions;

b. Performs this verification judicial branch entity-defined system transitional states or upon command by user with appropriate privilege on judicial branch entity-defined frequency;

c. Notifies judicial branch entity-defined personnel or roles of failed security verification tests; and

d. Shuts the information system down, restarts the information system, or other judicial branch entity-defined action when anomalies are discovered.

Recommendations: Transitional states for information systems include, for example, system startup, restart, shutdown, and abort. Notifications provided by information systems include, for example, electronic alerts to system administrators, messages to local computer consoles, and/or hardware indications such as lights.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD Not Selected	HIGH SI-6

21.7 SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY

Control: The judicial branch entity employs integrity verification tools to detect unauthorized changes to judicial branch entity-defined software, firmware, and information.

Recommendations: Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity (e.g., tampering). Software includes, for example, operating systems (with key internal components such as kernels, drivers), middleware, and applications. Firmware includes, for example, the Basic Input Output System (BIOS). Information includes metadata such as security attributes associated with information. State-of-the-practice integrity-checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and associated tools can automatically monitor the integrity of information systems and hosted applications.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD SI-7 (1) (7)	HIGH SI-7 (1) (2) (5) (7) (14)

21.8 SPAM PROTECTION

Control: The judicial branch entity:

a. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and

b. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

Recommendations: Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, mobile devices, and notebook/laptop computers. Spam can be transported by different means including, for example, electronic mail, electronic mail attachments, and web accesses. Spam protection mechanisms include, for example, signature definitions.

Priority and Baseline Allocation:

P2	LOW Not Selected	MOD SI-8 (1) (2)	HIGH SI-8 (1) (2)

21.9 INFORMATION INPUT VALIDATION

Control: The information system checks the validity of judicial branch entity-defined information inputs.

Recommendations: Checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, and acceptable values) verifies that inputs match specified definitions for format and content. Software 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 tainted output will perform the wrong operations or otherwise interpret the data incorrectly. Prescreening inputs prior to passing to interpreters prevents the content from being unintentionally interpreted as commands. Input validation helps to ensure accurate and correct inputs and prevent attacks such as cross-site scripting and a variety of injection attacks.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD SI-10	HIGH SI-10

21.10 ERROR HANDLING

Control: The information system:

a. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and

b. Reveals error messages only to judicial branch entity-defined personnel or roles.

Recommendations: Judicial branch entities carefully consider the structure/content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizational policy and operational requirements. Information that could be exploited by adversaries includes, for example, erroneous logon attempts with passwords entered by mistake as the username, mission/business information that can be derived from (if not stated explicitly by) information recorded, and personal information such as account numbers, social security numbers, and credit card numbers. In addition, error messages may provide a covert channel for transmitting information.

Priority and Baseline Allocation:

P2	LOW Not Selected	MOD SI-11	HIGH SI-11

21.11 INFORMATION HANDLING AND RETENTION

Control: The judicial branch entity handles and retains information within the information system and information output from the system in accordance with applicable federal and state laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

Recommendations: Information handling and retention requirements cover the full life cycle of information, in some cases extending beyond the disposal of information systems. The National Archives and Records Administration provides guidance on records retention.

Priority and Baseline Allocation:

P2	LOW SI-12	MOD SI-12	HIGH SI-12

21.12 MEMORY PROTECTION

Control: The information system implements judicial branch entity-defined security safeguards to protect its memory from unauthorized code execution.

Recommendations: Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can either be hardware-enforced or software-enforced with hardware providing the greater strength of mechanism.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD SI-16	HIGH SI-16

22.0 PRIVACY

22.1 AUTHORITY AND PURPOSE

22.1.1 Authority to Collect

Control: The judicial branch entity determines and documents the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information (PII), either generally or in support of a specific program or information system need.

Recommendations: Before collecting PII, the judicial branch entity determines whether the contemplated collection of PII is legally authorized. Program officials consult with the Senior Privacy Officer and legal counsel regarding the authority of any program or activity to collect PII. The authority to collect PII is documented in the System of Records Notice (SORN) and/or Privacy Impact Assessment (PIA) or other applicable documentation such as Privacy Act Statements or Computer Matching Agreements.

22.1.2 Purpose of Specification

Control: The judicial branch entity describes the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices.

Recommendations: Often, statutory language expressly authorizes specific collections and uses of PII. When statutory language is written broadly and thus subject to interpretation, organizations ensure, in consultation with the Senior Privacy Officer and legal counsel, that there is a close nexus between the general authorization and any specific collection of PII. Once the specific purposes have been identified, the purposes are clearly described in the related privacy compliance documentation, including but not limited to Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), and Privacy Act Statements provided at the time of collection (e.g., on forms organizations use to collect PII). Further, in order to avoid unauthorized collections or uses of PII, personnel who handle PII receive training on the organizational authorities for collecting PII, authorized uses of PII, and on the contents of the notice.

22.2 ACCOUNTABILITY, AUDIT, AND RISK MANAGEMENT

22.2.1 Governance and Privacy Program

Control: The judicial branch entity:

a. Appoints a Senior Privacy Officer accountable for developing, implementing, and maintaining a judicial branch entity-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information (PII) by programs and information systems;

b. Monitors federal privacy laws and policy for changes that affect the privacy program;

c. Allocates judicial branch entity-defined allocation of budget and staffing sufficient resources to implement and operate the organization-wide privacy program;

d. Develops a strategic judicial branch entity privacy plan for implementing applicable privacy controls, policies, and procedures;

e. Develops, disseminates, and implements judicial branch entity privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII; and

f. Updates privacy plan, policies, and procedures at least biennially.

Recommendations: The development and implementation of a comprehensive governance and privacy program demonstrates organizational accountability for and commitment to the protection of individual privacy. Accountability begins with the appointment of a Senior Privacy Officer with the authority, mission, resources, and responsibility to develop and implement a multifaceted privacy program. The Senior Privacy Officer, in consultation with legal counsel, information security officials, and others as appropriate: (i) ensures the development, implementation, and enforcement of privacy policies and procedures; (ii) defines roles and responsibilities for protecting PII; (iii) determines the level of information sensitivity with regard to PII holdings; (iv) identifies the laws, regulations, and internal policies that apply to the PII; (v) monitors privacy best practices; and (vi) monitors/audits compliance with identified privacy controls.

To further accountability, the Senior Privacy Officer develops privacy plans to document the privacy requirements of organizations and the privacy and security controls in place or planned for meeting those requirements. The plan serves as evidence of organizational privacy operations and supports resource requests by the Senior Privacy Officer. A single plan or multiple plans may be necessary depending upon the organizational structures, requirements, and resources, and the plan(s) may vary in comprehensiveness. For example, a one-page privacy plan may cover privacy policies, documentation, and controls already in place, such as Privacy Impact Assessments (PIA) and System of Records Notices (SORN). A comprehensive plan may include a baseline of privacy controls selected from this appendix and include: (i)

processes for conducting privacy risk assessments; (ii) templates and guidance for completing PIAs and SORNs; (iii) privacy training and awareness requirements; (iv) requirements for contractors processing PII; (v) plans for eliminating unnecessary PII holdings; and (vi) a framework for measuring annual performance goals and objectives for implementing identified privacy controls.

22.2.2 Privacy Impact and Risk Assessment

Control: The judicial branch entity:

a. Documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII); and

b. Conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, or any existing organizational policies and procedures.

Recommendations: Organizational privacy risk management processes operate across the life cycles of all mission/business processes that collect, use, maintain, share, or dispose of PII. The tools and processes for managing risk are specific to organizational missions and resources. They include, but are not limited to, the conduct of PIAs. The PIA is both a process and the document that is the outcome of that process. Some organizations may be required by law or policy to extend the PIA requirement to other activities involving PII or otherwise impacting privacy (e.g., programs, projects, or regulations). PIAs are conducted to identify privacy risks and identify methods to mitigate those risks. PIAs are also conducted to ensure that programs or information systems comply with legal, regulatory, and policy requirements. PIAs also serve as notice to the public of privacy practices. PIAs are performed before developing or procuring information systems, or initiating programs or projects, that collect, use, maintain, or share PII and are updated when changes create new privacy risks.

22.2.3 Privacy Requirements for Contractors and Service Providers

Control: The judicial branch entity:

a. Establishes privacy roles, responsibilities, and access requirements for contractors and service providers; and

b. Includes privacy requirements in contracts and other acquisition-related documents.

Recommendations: Contractors and service providers include, but are not limited to, information providers, information processors, and other organizations providing information system development, information technology services, and other

outsourced applications. Judicial branch entities consult with legal counsel, the Senior Privacy Officer, and contracting officers about applicable laws, directives, policies, or regulations that may impact implementation of this control.

22.2.4 Privacy Monitoring and Auditing

Control: The judicial branch entity monitors and audits privacy controls and internal privacy policy annually to ensure effective implementation.

Recommendations: To promote accountability, judicial branch entities identify and address gaps in privacy compliance, management, operational, and technical controls by conducting regular assessments (e.g., internal risk assessments). These assessments can be self-assessments or third-party audits that result in reports on compliance gaps identified in programs, projects, and information systems. In addition to auditing for effective implementation of all privacy controls identified in this appendix, judicial branch entities assess whether they: (i) implement a process to embed privacy considerations into the life cycle of personally identifiable information (PII), programs, information systems, mission/business processes, and technology; (ii) monitor for changes to applicable privacy laws, regulations, and policies; (iii) track programs, information systems, and applications that collect and maintain PII to ensure compliance; (iv) ensure that access to PII is only on a need-to-know basis; and (v) ensure that PII is being maintained and used only for the legally authorized purposes identified in the public notice(s).

Judicial branch entities also: (i) implement technology to audit for the security, appropriate use, and loss of PII; (ii) perform reviews to ensure physical security of documents containing PII; (iii) assess contractor compliance with privacy requirements; and (iv) ensure that corrective actions identified as part of the assessment process are tracked and monitored until audit findings are corrected. The judicial branch entity Senior Privacy Officer coordinates monitoring and auditing efforts with information security officials and ensures that the results are provided to senior managers and oversight officials.

22.2.5 Privacy Awareness and Training

Control: The judicial branch entity:

a. Develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures;

b. Administers basic privacy training annually and targeted, role-based privacy training for personnel having responsibility for personally identifiable information (PII) or for activities that involve PII at least annually; and

c. Ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements at least annually.

Recommendations: Through implementation of a privacy training and awareness strategy, the judicial branch entity promotes a culture of privacy. Privacy training and awareness programs typically focus on broad topics, such as responsibilities under the Privacy Act of 1974 and the consequences of failing to carry out those responsibilities, how to identify new privacy risks, how to mitigate privacy risks, and how and when to report privacy incidents. Privacy training may also target data collection and use requirements identified in public notices, such as Privacy Impact Assessments (PIAs) or System of Records Notices (SORNs) for a program or information system. Specific training methods may include: (i) mandatory annual privacy awareness training; (ii) targeted, role-based training; (iii) internal privacy program websites; (iv) manuals, guides, and handbooks; (v) slide presentations; (vi) events (e.g., privacy awareness week, privacy clean-up day); (vii) posters and brochures; and (viii) email messages to all employees and contractors. Judicial branch entities update training based on changing statutory, regulatory, mission, program, business process, and information system requirements, or on the results of compliance monitoring and auditing. Where appropriate, Judicial branch entities may provide privacy training as part of existing information security training.

22.2.6 Privacy Reporting

Control: The judicial branch entity develops, disseminates, and updates reports to the oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.

Recommendations: Through internal and external privacy reporting, judicial branch entities promote accountability and transparency in organizational privacy operations. Reporting also helps judicial branch entities to determine progress in meeting privacy compliance requirements and privacy controls, compare performance across the federal government, identify vulnerabilities and gaps in policy and implementation, and identify success models. Types of privacy reports include: (i) annual Senior Privacy Officer reports to the Executive Board; (ii) other public reports required by specific statutory mandates or internal policies of judicial branch entities. The judicial branch entity Senior Privacy Officer consults with legal counsel, where appropriate, to ensure that organizations meet all applicable privacy reporting requirements.

22.2.7 Privacy-Enhanced System Design and Development

Control: The judicial branch entity designs information systems to support privacy by automating privacy controls.

Recommendations: To the extent feasible, when designing organizational information systems, judicial branch entities employ technologies and system capabilities that automate privacy controls on the collection, use, retention, and disclosure of personally identifiable information (PII). By building privacy controls into system design and development, judicial branch entities mitigate privacy risks to PII, thereby reducing the likelihood of information system breaches and other privacy-related incidents. Judicial branch entities also conduct periodic reviews of systems to determine the need for updates to maintain compliance with the Privacy Act and the judicial branch entity's privacy policy. Regardless of whether automated privacy controls are employed, judicial branch entities regularly monitor information system use and sharing of PII to ensure that the use/sharing is consistent with the authorized purposes identified in the Privacy Act and/or in the public notice of judicial branch entities, or in a manner compatible with those purposes.

22.2.8 Accounting of Disclosures

Control: The judicial branch entity:

a. Keeps an accurate accounting of disclosures of information held in each system of records under its control, including:

    1. Date, nature, and purpose of each disclosure of a record; and

    2. Name and address of the person or agency to which the disclosure was made;

b. Retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer; and

c. Makes the accounting of disclosures available to the person named in the record upon request.

Recommendations: The Senior Privacy Officer periodically consults with managers of judicial branch entity systems of record to ensure that the required accountings of disclosures of records are being properly maintained and provided to persons named in those records consistent with the dictates of the Privacy Act. Judicial branch entities are not required to keep an accounting of disclosures when the disclosures are made to individuals with a need to know, are made pursuant to applicable statutes. Heads of agencies can promulgate rules to exempt certain systems of records from the requirement to provide the accounting of disclosures to individuals.

22.3 DATA QUALITY AND INTEGRITY

22.3.1 Data Quality

Control: The judicial branch entity:

a. Confirms to the greatest extent practicable upon collection or creation of personally identifiable information (PII), the accuracy, relevance, timeliness, and completeness of that information;

b. Collects PII directly from the individual to the greatest extent practicable;

c. Checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems judicial branch entity-defined frequency; and

d. Issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

Recommendations: Judicial branch entities take reasonable steps to confirm the accuracy and relevance of PII. Such steps may include, for example, editing and validating addresses as they are collected or entered into information systems using automated address verification look-up application programming interfaces (API). The types of measures taken to protect data quality are based on the nature and context of the PII, how it is to be used, and how it was obtained. Measures taken to validate the accuracy of PII that is used to make determinations about the rights, benefits, or privileges of individuals under federal and state programs may be more comprehensive than those used to validate less sensitive PII. Additional steps may be necessary to validate PII that is obtained from sources other than individuals or the authorized representatives of individuals.

When PII is of a sufficiently sensitive nature (e.g., when it is used for annual reconfirmation of a taxpayer's income for a recurring benefit), judicial branch entities incorporate mechanisms into information systems and develop corresponding procedures for how frequently, and by what method, the information is to be updated.

22.3.2 Data Integrity and Data Integrity Board

Control: The judicial branch entity:

a. Documents processes to ensure the integrity of personally identifiable information (PII) through existing security controls; and

b. Where applicable, establishes a Data Integrity Board when appropriate to oversee organizational Computer Matching Agreements and to ensure that those agreements comply with the computer matching provisions of the Privacy Act.

Recommendations: Before collecting PII, the organization determines whether the contemplated collection of PII is legally authorized. Program officials consult with the Senior Privacy Officer and legal counsel regarding the authority of any program or activity to collect PII. The authority to collect PII is documented in the System of

Records Notice (SORN) and/or Privacy Impact Assessment (PIA) or other applicable documentation such as Privacy Act Statements or Computer Matching Agreements.

22.4 DATA MINIMIZATION AND RETENTION

22.4.1 Minimization of Personally Identifiable Information

Control: The judicial branch entity:

a. Identifies the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection;

b. Limits 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. Conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings at least annually 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.

Recommendations: Judicial branch entities take appropriate steps to ensure that the collection of PII is consistent with a purpose authorized by law or regulation. The minimum set of PII elements required to support a specific judicial branch entity business process may be a subset of the PII the judicial branch entity is authorized to collect. Program officials consult with the Senior Privacy Officer and legal counsel to identify the minimum PII elements required by the information system or activity to accomplish the legally authorized purpose.

Judicial branch entities can further reduce their privacy and security risks by also reducing their inventory of PII, where appropriate.

By performing periodic evaluations, judicial branch entities reduce risk, ensure that they are collecting only the data specified in the notice, and ensure that the data collected is still relevant and necessary for the purpose(s) specified in the notice.

22.4.2 Data Retention and Disposal

Control: The judicial branch entity:

a. Retains each collection of personally identifiable information (PII) for judicial branch entity-defined time period to fulfill the purpose(s) identified in the notice or as required by law;

b. Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a judicial branch entity-approved record retention

schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and

c. Uses judicial branch entity-defined techniques or methods to ensure secure deletion or destruction of PII (including originals, copies, and archived records).

Recommendations: The judicial branch entity provides retention schedules that govern the disposition of judicial branch entity records. Program officials coordinate with records officers to identify appropriate retention periods and disposal methods. Methods of storage include, for example, electronic, optical media, or paper.

Examples of ways judicial branch entities may reduce holdings include reducing the types of PII held (e.g., delete Social Security numbers if their use is no longer needed) or shortening the retention period for PII that is maintained if it is no longer necessary to keep PII for long periods of time (this effort is undertaken in consultation with an organization's records officer). In both examples, judicial branch entities provide notice (e.g., an updated System of Records Notice) to inform the public of any changes in holdings of PII.

Certain read-only archiving techniques, such as DVDs, CDs, microfilm, or microfiche, may not permit the removal of individual records without the destruction of the entire database contained on such media.

22.4.3 Minimization of PII Used in Testing, Training, and Research

Control: The judicial branch:

a. Develops policies and procedures that minimize the use of personally identifiable information (PII) for testing, training, and research; and

b. Implements controls to protect PII used for testing, training, and research.

Recommendations: Judicial branch entities often use PII for testing new applications or information systems prior to deployment. Judicial branch entities also use PII for research purposes and for training. The use of PII in testing, research, and training increases risk of unauthorized disclosure or misuse of the information. If PII must be used, judicial branch entities take measures to minimize any associated risks and to authorize the use of and limit the amount of PII for these purposes. Judicial branch entities consult with the Security Privacy Officer and legal counsel to ensure that the use of PII in testing, training, and research is compatible with the original purpose for which it was collected.

22.5 INDIVIDUAL PARTICIPATION AND REDRESS

22.5.1 Consent

Control: The judicial branch:

a. Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection;

b. Provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII;

c. Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and

d. Ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.

Recommendations: Consent is fundamental to the participation of individuals in the decision-making process regarding the collection and use of their PII and the use of technologies that may increase risk to personal privacy. To obtain consent, judicial branch entities provide individuals appropriate notice of the purposes of the PII collection or technology use and a means for individuals to consent to the activity. Judicial branch entities tailor the public notice and consent mechanisms to meet operational needs. Judicial branch entities achieve awareness and consent, for example, through updated public notices.

Judicial branch entities may obtain consent through opt-in, opt-out, or implied consent. Opt-in consent is the preferred method, but it is not always feasible. Opt-in requires that individuals take affirmative action to allow organizations to collect or use PII. For example, opt-in consent may require an individual to click a radio button on a website, or sign a document providing consent. In contrast, opt-out requires individuals to take action to prevent the new or continued collection or use of such PII. Implied consent occurs where individuals' behavior or failure to object indicates agreement with the collection or use of PII (e.g., by entering and remaining in a building where notice has been posted that security cameras are in use, the individual implies consent to the video recording). Depending upon the nature of the program or information system, it may be appropriate to allow individuals to limit the types of PII they provide and subsequent uses of that PII. Organizational consent mechanisms include a discussion of the consequences to individuals of failure to provide PII. Consequences can vary from organization to organization.

22.5.2 Individual Access

Control: The judicial branch entity:

a. Provides individuals the ability to have access to their personally identifiable information (PII) maintained in its system(s) of records;

b. Publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records;

c. Publishes access procedures in System of Records Notices (SORNs); and

d. Adheres to Privacy Act requirements and judicial branch entity policies and guidance for the proper processing of Privacy Act requests.

Recommendations: Before collecting PII, the judicial branch entity determines whether the contemplated collection of PII is legally authorized. Program officials consult with the Senior Privacy Officer and legal counsel regarding the authority of any program or activity to collect PII. The authority to collect PII is documented in the System of Records Notice (SORN) and/or Privacy Impact Assessment (PIA) or other applicable documentation such as Privacy Act Statements.

22.5.3 Redress

Control: The judicial branch entity:

a. Provides a process for individuals to have inaccurate personally identifiable information (PII) maintained by the judicial branch entity corrected or amended, as appropriate; and

b. Establishes a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information-sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended.

Recommendations: Redress supports the ability of individuals to ensure the accuracy of PII held by the judicial branch entity. Effective redress processes demonstrate organizational commitment to data quality especially in those business functions where inaccurate data may result in inappropriate decisions or denial of benefits and services to individuals. Judicial branch entities use discretion in determining if records are to be corrected or amended, based on the scope of redress requests, the changes sought, and the impact of the changes. Individuals may appeal an adverse decision and have incorrect information amended, where appropriate.

To provide effective redress, judicial branch entities: (i) provide effective notice of the existence of a PII collection; (ii) provide plain language explanations of the processes and mechanisms for requesting access to records; (iii) establish criteria for submitting requests for correction or amendment; (iv) implement resources to analyze and

adjudicate requests; (v) implement means of correcting or amending data collections; and (vi) review any decisions that may have been the result of inaccurate information.

22.5.4 Complaint Management

Control: The judicial branch entity implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.

Recommendations: Complaints, concerns, and questions from individuals can serve as a valuable source of external input that ultimately improves operational models, uses of technology, data collection practices, and privacy and security safeguards. Judicial branch entities provide complaint mechanisms that are readily accessible by the public, include all information necessary for successfully filing complaints (including contact information for the Senior Privacy Officer or other official designated to receive complaints), and are easy to use. Organizational complaint management processes include tracking mechanisms to ensure that all complaints received are reviewed and appropriately addressed in a timely manner.

22.6 SECURITY

22.6.1 Inventory of Personally Identifiable Information

Control: The judicial branch entity:

a. Establishes, maintains, and updates annually an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII); and

b. Provides each update of the PII inventory to the information security official annually to support the establishment of information security requirements for all new or modified information systems containing PII.

Recommendations: The PII inventory enables judicial branch entities to implement effective administrative, technical, and physical security policies and procedures to protect PII consistent with Appendix F in NIST SP 800-53, and to mitigate risks of PII exposure. As one method of gathering information for their PII inventories, judicial branch entities may extract the following information elements from Privacy Impact Assessments (PIA) for information systems containing PII: (i) the name and acronym for each system identified; (ii) the types of PII contained in that system; (iii) classification of level of sensitivity of all types of PII, as combined in that information system; and (iv) classification of level of potential risk of substantial harm, embarrassment, inconvenience, or unfairness to affected individuals, as well as the financial or reputational risks to organizations, if PII is exposed. Judicial branch

entities take due care in updating the inventories by identifying linkable data that could create PII.

22.6.2 Privacy Incident Response

Control: The judicial branch entity:

a. Develops and implements a Privacy Incident Response Plan; and

b. Provides an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan.

Recommendations: In contrast to the Incident Response (IR) family in Appendix F in NIST SP 800-53, which concerns a broader range of incidents affecting information security, this control uses the term Privacy Incident to describe only those incidents that relate to personally identifiable information (PII). The judicial branch entity Privacy Incident Response Plan is developed under the leadership of the Senior Privacy Officer. The plan includes: (i) the establishment of a cross-functional Privacy Incident Response Team that reviews, approves, and participates in the execution of the Privacy Incident Response Plan; (ii) a process to determine whether notice to oversight organizations or affected individuals is appropriate and to provide that notice accordingly; (iii) a privacy risk assessment process to determine the extent of harm, embarrassment, inconvenience, or unfairness to affected individuals and, where appropriate, to take steps to mitigate any such risks; (iv) internal procedures to ensure prompt reporting by employees and contractors of any privacy incident to information security officials and the Senior Privacy Officer, consistent with organizational incident management structures; and (v) internal procedures for reporting noncompliance with organizational privacy policy by employees or contractors to appropriate management or oversight officials. Some judicial branch entities may be required by law or policy to provide notice to oversight organizations in the event of a breach. Judicial branch entities may also choose to integrate Privacy Incident Response Plans with Security Incident Response Plans, or keep the plans separate.

22.7 TRANSPARENCY

22.7.1 Privacy Notice

Control: The judicial branch entity:

a. Provides effective notice to the public and to individuals regarding: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII); (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how the judicial branch entity uses PII and the consequences of exercising or not

exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary;

b. Describes: (i) the PII the judicial branch entity collects and the purpose(s) for which it collects that information; (ii) how the organization uses PII internally; (iii) whether the judicial branch entity shares PII with external entities, the categories of those entities, and the purposes for such sharing; (iv) whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; (v) how individuals may obtain access to PII; and (vi) how the PII will be protected; and

c. Revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change.

Recommendations: Effective notice, by virtue of its clarity, readability, and comprehensiveness, enables individuals to understand how an organization uses PII generally and, where appropriate, to make an informed decision prior to providing PII to an organization. Effective notice also demonstrates the privacy considerations that the judicial branch entity has addressed in implementing its information practices. The judicial branch entity may provide general public notice through a variety of means, as required by law or policy, including System of Records Notices (SORNs), Privacy Impact Assessments (PIAs), or in a website privacy policy. As required by the Privacy Act, the judicial branch entity also provides direct notice to individuals via Privacy Act Statements on the paper and electronic forms it uses to collect PII, or on separate forms that can be retained by the individuals.

The judicial branch entity Senior Privacy Officer is responsible for the content of the judicial branch entity's public notices, in consultation with legal counsel and relevant program managers. The public notice requirement in this control is satisfied by an organization's compliance with the public notice provisions of the Privacy Act. Changing PII practice or policy without prior notice is disfavored and should only be undertaken in consultation with the Senior Privacy Officer and counsel.

22.7.2 System of Records Notices and Privacy Act Statements

Control: The judicial branch entity:

a. Where applicable, publishes System of Records Notices (SORNs) in the Federal Register, subject to required oversight processes, for systems containing personally identifiable information (PII);

b. Keeps SORNs current; and

c. Includes Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.

Recommendations: Judicial branch entities issue SORNs to provide the public notice regarding PII collected in a system of records, which the Privacy Act defines as "a group of any records under the control of any agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifier." SORNs explain how the information is used, retained, and may be corrected, and whether certain portions of the system are subject to Privacy Act exemptions for law enforcement. Privacy Act Statements provide notice of: (i) the authority of organizations to collect PII; (ii) whether providing PII is mandatory or optional; (iii) the principal purpose(s) for which the PII is to be used; (iv) the intended disclosures (routine uses) of the information; and (v) the consequences of not providing all or some portion of the information requested. When information is collected verbally, judicial branch entities read a Privacy Act Statement prior to initiating the collection of PII (for example, when conducting telephone interviews or surveys).

22.7.3 Dissemination of Privacy Program Information

Control: The judicial branch entity:

a. Ensures that the public has access to information about its privacy activities and is able to communicate with its Senior Privacy Officer; and

b. Ensures that its privacy practices are publicly available through organizational websites or otherwise.

Recommendations: Judicial branch entities employ different mechanisms for informing the public about their privacy practices including, but not limited to, Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), privacy reports, publicly available web pages, email distributions, blogs, and periodic publications (e.g., quarterly newsletters). Judicial branch entities also employ publicly facing email addresses and/or phone lines that enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices.

22.8 USE LIMITATION

22.8.1 Internal Use

Control: The judicial branch entity uses personally identifiable information (PII) internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.

Recommendations: Judicial branch entities take steps to ensure that they use PII only for legally authorized purposes and in a manner compatible with uses identified in the Privacy Act and/or in public notices. These steps include monitoring and auditing organizational use of PII and training organizational personnel on the authorized uses of PII. With guidance from the Senior Privacy Officer and where appropriate, legal counsel, judicial branch entities document processes and procedures for evaluating any proposed new uses of PII to assess whether they fall within the scope of the organizational authorities. Where appropriate, judicial branch entities obtain consent from individuals for the new use(s) of PII.

22.8.2 Information Sharing with Third Parties

Control: The judicial branch entity:

a. Shares personally identifiable information (PII) externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes;

b. Where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used;

c. Monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and

d. Evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

Recommendations: The judicial branch entity Senior Privacy Officer and, where appropriate, legal counsel review and approve any proposed external sharing of PII, including with other public, international, or private sector entities, for consistency with uses described in the existing organizational public notice(s). When a proposed new instance of external sharing of PII is not currently authorized by the Privacy Act and/or specified in a notice, judicial branch entities evaluate whether the proposed external sharing is compatible with the purpose(s) specified in the notice. If the proposed sharing is compatible, judicial branch entities review, update, and republish their Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), website privacy policies, and other public notices, if any, to include specific descriptions of the new uses(s) and obtain consent where appropriate and feasible. Information-sharing agreements also include security protections consistent with the sensitivity of the information being shared.