SAM – INFORMATION SECURITY
(Office of Information Security)

Note: Effective January 1, 2008, the California Information Security restructured and renumbered the content of this chapter and moved it from SAM Sections 4840 – 4845 to SAM Sections 5300 – 5399. See the Government Online Responsible Information Management (GO RIM) web site at www.infosecurity.ca.gov for statewide authority, standards, guidance, forms, and tools for information security activities.

CHAPTER 5300 INDEX

INTRODUCTION	**5300**
ARRANGEMENT OF CHAPTER	**5300.1**
GOVERNING PROVISIONS	**5300.2**
APPLICABILITY	**5300.3**
DEFINITIONS	**5300.4**
MINIMUM SECURITY CONTROLS	**5300.5**
INFORMATION SECURITY PROGRAM	**5305**
INFORMATION SECURITY PROGRAM MANAGEMENT	**5305.1**
POLICY, PROCEDURE AND STANDARDS MANAGEMENT	**5305.2**
INFORMATION SECURITY ROLES AND RESPONSIBILITIES	**5305.3**
PERSONNEL MANAGEMENT	**5305.4**
INFORMATION ASSET MANAGEMENT	**5305.5**
RISK MANAGEMENT	**5305.6**
RISK ASSESSMENT	**5305.7**
PROVISIONS FOR AGREEMENTS WITH STATE AND NON-STATE ENTITIES	**5305.8**
INFORMATION SECURITY PROGRAM METRIC	**5305.9**
PRIVACY	**5310**
STATE ENTITY PRIVACY STATEMENT AND NOTICE ON COLLECTION	**5310.1**
LIMITING COLLECTION	**5310.2**
LIMITING USE AND DISCLOSURE	**5310.3**
INDIVIDUAL ACCESS TO PERSONAL INFORMATION	**5310.4**
INFORMATION INTEGRITY	**5310.5**

(Continued)

(Continued)

CHAPTER 5300 INDEX (Cont. 1)

DATA RETENTION AND DESTRUCTION	5310.6
SECURITY SAFEGUARDS	5310.7
INFORMATION SECURITY INTEGRATION	5315
SYSTEM AND SERVICES ACQUISITION	5315.1
SYSTEM DEVELOPMENT LIFECYCLE	5315.2
INFORMATION ASSET DOCUMENTATION	5315.3
SYSTEM DEVELOPER SECURITY TESTING	5315.4
CONFIGURATION MANAGEMENT	5315.5
ACTIVATE ONLY ESSENTIAL FUNCTIONALITY	5315.6
SOFTWARE USAGE RESTRICTIONS	5315.7
INFORMATION ASSET CONNECTIONS	5315.8
SECURITY AUTHORIZATION	5315.9
TRAINING AND AWARENESS FOR INFORMATION SECURITY AND PRIVACY	5320
SECURITY AND PRIVACY AWARENESS	5320.1
SECURITY AND PRIVACY AWARENESS TRAINING	5320.2
SECURITY AND PRIVACY AWARENESS TRAINING RECORDS	5320.3
PERSONNEL SECURITY	5320.4
BUSINESS CONTINUITY WITH TECHNOLOGY RECOVERY	5325
TECHNOLOGY RECOVERY PLAN	5325.1
TECHNOLOGY RECOVERY TRAINING	5325.2
TECHNOLOGY RECOVERY TESTING	5325.3
ALTERNATE STORAGE AND PROCESSING SITE	5325.4
TELECOMMUNICATIONS SERVICES	5325.5
INFORMATION SYSTEM BACKUPS	5325.6

(Continued)

(Continued)

CHAPTER 5300 INDEX (Cont. 2)

INFORMATION SECURITY COMPLIANCE	**5330**
SECURITY ASSESSMENTS	**5330.1**
COMPLIANCE REPORTING	**5330.2**
INFORMATION SECURITY MONITORING	**5335**
CONTINUOUS MONITORING	**5335.1**
AUDITABLE EVENTS	**5335.2**
INFORMATION SECURITY INCIDENT MANAGEMENT	**5340**
INCIDENT RESPONSE TRAINING	**5340.1**
INCIDENT RESPONSE TESTING	**5340.2**
INCIDENT HANDLING	**5340.3**
INCIDENT REPORTING	**5340.4**
VULNERABILITY AND THREAT MANAGEMENT	**5345**
OPERATIONAL SECURITY	**5350**
ENCRYPTION	**5350.1**
ENDPOINT DEFENSE	**5355**
MALICIOUS CODE PROTECTION	**5355.1**
SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	**5355.2**
IDENTITY AND ACCESS MANAGEMENT	**5360**
REMOTE ACCESS	**5360.1**
WIRELESS ACCESS	**5360.2**
PHYSICAL SECURITY	**5365**
ACCESS CONTROL FOR OUTPUT DEVICES	**5365.1**
MEDIA PROTECTION	**5365.2**
MEDIA DISPOSAL	**5365.3**

INTRODUCTION 5300

(Revised 12/13)

Information security refers to the protection of information, information systems, equipment, software, and people from a wide spectrum of threats and risks. Implementing appropriate security measures and controls to provide for the confidentiality, integrity, and availability of information, regardless of its form (electronic, optical, oral, print, or other media), is critical to ensure business continuity, and protect information assets against unauthorized access, use, disclosure, disruption, modification, or destruction. Information security is also the means by which privacy of personal information held by state entities is protected.

The state's information assets, including its data processing capabilities, information technology infrastructure and data are an essential public resource. For many state entities, program operations would effectively cease in the absence of key computer systems. In some cases, public health and safety would be immediately jeopardized by the failure or disruption of a system. The non-availability of state information systems and resources can also have a detrimental impact on the state economy and the citizens who rely on state programs. Furthermore, the unauthorized acquisition, access, modification, deletion, or disclosure of information included in state entity files and databases can compromise the integrity of state programs, violate individual right to privacy, and constitute a criminal act.

ARRANGEMENT OF CHAPTER 5300.1

(Revised 12/13)

This Chapter and its corresponding sections are organized as follows:

Introduction: A brief description introducing the section, when necessary.

Policy: A clear and unambiguous “Policy” statement which directs state entities at a high level as to required actions and outcomes.

Governing Provisions: Identifies any additional overarching laws, regulations or policies governing or related to the specific policy requirement.

Implementation Controls: Refers to the standards, instructions, procedures, and forms directing state entities in the “how” to comply with policy set forth in this Chapter.

GOVERNING PROVISIONS **5300.2**
(Revised 6/14)

Policy: As set forth in Government Code section 11549.3, state entities shall comply with the information security and privacy policies, standards and procedures issued by the California Information Security Office (CISO). In addition to compliance with the information security and privacy policies, standards, procedures, and filing requirements issued by the CISO, state entities shall ensure compliance with all security and privacy laws, regulations, rules, and standards specific to and governing the administration of their programs. Program administrators shall work with their general counsel, Information Security Officer (ISO), and Privacy Program Officer/Coordinator to identify all security and privacy requirements applicable to their programs and ensure implementation of the requisite controls.

Governing Provisions: Government Code section 11549.3 provides the CISO with the responsibility and authority to create, issue, and maintain policies, standards, and procedures; direct each state entity to effectively manage risk; advise and consult with each state entity on security issues; and ensure each state entity is in compliance with the requirements specified in the State Administrative Manual (SAM) Chapter 5300.

Government Code section 11549.3 also provides the CISO with the responsibility to coordinate the activities of state entity ISOs for purposes of integrating statewide security initiatives and ensuring compliance with information security and privacy policies and standards. The CISO is also provided with the authority to conduct, or require to be conducted, independent security assessments or audits of any entity. The cost of such assessments or audits shall be funded by the state entity being assessed or audited.

(Continued)

(Continued)
GOVERNING PROVISIONS **5300.2 (Cont. 1)**
(Revised 6/14)

Many information security and privacy requirements are program specific; thus, the legal and regulatory requirements may vary from one program to another. For example, the laws governing security and privacy for health care programs differ from the laws governing energy programs. The following overarching laws, which affect the categorization, classification, protection, and dissemination of information, are applicable to most state entities:

1. Article 1, Section 1, of the Constitution of the State of California defines pursuing and obtaining privacy as an inalienable right.
2. The Information Practices Act of 1977 (Civil Code section 1798, et seq.) places specific requirements on each state entity in the collection, use, maintenance, and dissemination of information relating to individuals.
3. The California Public Records Act (Government Code sections 6250-6265) provides for the inspection of public records and authorizes specific exemptions for not disclosing certain records or portions of certain records.
4. The State Records Management Act (Government Code sections 14740-14770) provides for the application of management methods to the creation, utilization, maintenance, retention, preservation, and disposal of state records, including determination of records essential to the continuation of state government in the event of a major disaster. (SAM sections 1601 through 1699 contain administrative regulations in support of the Records Management Act.)
5. The Comprehensive Computer Data Access and Fraud Act (Penal Code section 502) affords protection to individuals, businesses, and governmental entities from tampering, interference, damage, and unauthorized access to computer data and computer systems. It allows for civil action against any person convicted of violating the criminal provisions for compensatory damages.

APPLICABILITY 5300.3

(Revised 12/13)

Policy: SAM Chapter 5300 shall apply to the following:

1. All state entities unless otherwise specifically exempted by law or state policy.
2. All categories of automated and paper information, including, but not limited to, records, files, and databases.
3. Information technology facilities, software, and equipment, including personal computer systems owned or leased by state entities.

For the purposes of this Chapter, the term "state entity" shall denote a State of California agency, department, office, board, bureau, or other distinct governmental organization in the executive branch. Where a requirement, obligation, or responsibility is assigned to a state entity, the state entity head shall accept or delegate that requirement to an individual or individuals fully qualified to effectively ensure compliance with the requirement, and ensure the obligation and responsibility is met. Ultimately, the state entity head shall be responsible for policy compliance.

DEFINITIONS 5300.4

(Revised 12/13)

Policy: Each state entity shall use the information security and privacy definitions issued by the CISO in implementing information security and privacy policy in their daily operations. The definitions are located on the CISO website at http://www.cio.ca.gov/OIS/Government/definitions.asp.

MINIMUM SECURITY CONTROLS **5300.5**
(Revised 12/13)

Policy: California has adopted the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 as minimum information security control requirements to support implementation and compliance with the Federal Information Processing Standards (FIPS). Each state entity shall use the FIPS and NIST SP 800-53 in the planning, development, implementation, and maintenance of their information security programs. Adoption of these standards will facilitate a more consistent, comparable, and repeatable approach for securing state assets; and, create a foundation from which standardized assessment methods and procedures may be used to measure security program effectiveness.

The CISO has also adopted additional standards and procedures to address more specific requirements or needs unique to California. These additional standards are referenced in the applicable policy section and maintained in the Statewide Information Management Manual (SIMM).

Governing Provisions: SAM section 5100 requires state entities to use the American National Standards Institute (ANSI) and the FIPS standards in their information management planning and operations.

Implementation Controls: ANSI; FIPS; NIST SP 800-53

INFORMATION SECURITY PROGRAM 5305

(Revised 6/14)

Policy: Each state entity is responsible for establishing an information security program. The program shall include planning, oversight, and coordination of its information security program activities to effectively manage risk, provide for the protection of information assets, and prevent illegal activity, fraud, waste, and abuse in the use of information assets.

Each state entity shall:

1. Align the information security program, its activities, and staff with the requirements of this Chapter;
2. Establish a governance body to direct the development of state entity specific information security plans, policies, standards, and other authoritative documents;
3. Oversee the creation, maintenance, and enforcement of established information security policies, standards, procedures, and guidelines;
4. Ensure the state entity's security policies and procedures are fully documented and state entity staff is aware of, has agreed to comply with, and understands the consequences of failure to comply with policies and procedures;
5. Identify and integrate or align information security goals and objectives to the state entity's strategic and tactical plans;
6. Develop and track information security and privacy risk key performance indicators;
7. Develop and disseminate security and privacy metrics and risk information to state entity executives and other managers for decision making purposes; and
8. Coordinate state entity security efforts with local government entities and other branches of government as applicable.

Implementation Controls: NIST SP 800-53: Planning (PL); Program Management (PM)

INFORMATION SECURITY PROGRAM MANAGEMENT 5305.1

(Revised 6/14)

Policy: Each state entity must provide for the proper use and protection of its information assets. Accordingly each state entity shall:

1. Develop, implement, and maintain a state entity-wide Information Security Program Plan.
2. Ensure the plan documentation provides the following:
    a. an overview of the requirements for the state entity's information security program;
    b. a description of the state entity's strategy and prioritization approach to information security, privacy, and risk management;
    c. a plan for integrating information security resource needs into the state entity's capital planning and funding request processes; and
    d. a plan of action and milestones process for addressing program deficiencies.
3. Be approved and disseminated by the state entity head responsible and accountable for risks incurred to the state entity's mission, functions, assets, image and reputation.
4. Identify roles and responsibilities, and assign management responsibilities for information security program management consistent with the roles and responsibilities described in the Information Security Program Management Standard (SIMM 5305-A).

Implementation Controls: NIST SP 800-53: Planning (PL); Program Management (PM); Information Security Program Management Standard (SIMM 5305-A)

POLICY, PROCEDURE AND STANDARDS MANAGEMENT **5305.2**
(Revised 6/14)

Policy: Each state entity must provide for the protection of its information assets by establishing appropriate administrative, operational and technical policies, standards, and procedures to ensure its operations conform with business requirements, laws, and administrative policies, and personnel maintain a standard of due care to prevent misuse, loss, disruption or compromise of state entity information assets. Each state entity shall adopt, maintain and enforce internal administrative, operational and technical policies, standards and procedures in accordance with SIMM 5305-A to support information security program plan goals and objectives.

Implementation Controls: NIST SP 800-53: Planning (PL); Program Management (PM); SIMM 5305-A

INFORMATION SECURITY ROLES AND RESPONSIBILITIES **5305.3**
(Revised 6/14)

Policy: Information security is a shared responsibility. All personnel have a role and responsibility in the proper use and protection of state information assets. Each state entity shall ensure information security program roles and responsibilities identified in SIMM 5305-A are acknowledged and understood by all state entity personnel.

Implementation Controls: NIST SP 800-53: Planning (PL); Program Management (PM); SIMM 5305-A

PERSONNEL MANAGEMENT **5305.4**
(Revised 12/13)

Policy: Each state entity must identify security and privacy roles and responsibilities for all personnel. This will ensure personnel are informed of their roles and responsibilities for using state entity information assets, to reduce the risk of inappropriate use, and a documented process to remove access when changes occur. Personnel practices related to security management must include:

1. Employment history, fingerprinting, and/or criminal background checks on personnel who work with or have access to confidential, personal, or sensitive information or critical applications may be necessary for a particular state entity. Each state entity should consult the California Human Resources Department and the Department of Justice for specific rules and regulations relative to employment history, fingerprinting, or criminal background checks.
2. Initial training of state entity personnel with respect to individual, state entity, and statewide security and privacy responsibilities and policies before being granted access to information assets, and annually thereafter.
3. Signing of acknowledgments of security and privacy responsibility by all personnel.
4. Transfer procedures that ensure access rights and permissions to state entity information assets are reviewed for appropriateness and reauthorized by program management when personnel is transferred within the state entity, so that access to information assets is limited to that which is needed by personnel in the performance of their job-related duties.
5. Termination procedures that ensure state entity information assets are not accessible to separated personnel.

INFORMATION ASSET MANAGEMENT **5305.5**
(Revised 6/14)

Introduction: In order to provide for the proper use and protection of information assets, the value and level of protection needed must be clearly specified and understood.

Policy: Each state entity must understand the value of its information assets and the level of protection those assets require. To this end, each state entity shall establish and maintain an inventory of all of its information assets, including information systems, information system components, and information repositories (both electronic and paper). The inventory shall contain a listing of all programs and information systems identified as collecting, using, maintaining, or sharing state entity information. The inventory must include categorization and classification of the information assets by program management, and based on the Information Security Program Management Standard (SIMM 5305-A), California Public Records Act (Government Code sections 6250-6265), Information Practices Act of 1977 (Civil Code Section 1798, et seq.), FIPS Publication 199, and laws governing administration of the state entity's programs.

The categorization and classification of information assets shall be used in the determination of an asset's needed level of protection. If the information asset's level of protection is not clear, the state entity is to protect the asset to the categorization level of "Moderate" as defined by FIPS Publication 199. Where the state entity is the custodian or user of the information asset, and not the owner, as in the case of Federal Tax Information, Criminal Justice Information Services information, and so forth the state entity shall ensure the data owner specifies the level of protection. The state entity shall adhere to the data owner's classification and level of protection requirements.

Each information asset for which the state entity has ownership responsibility shall be inventoried and identified to include the following:

1. Description and value of the information asset.
2. Owner of the information asset.
3. Custodians of the information asset.
4. Users of the information asset.
5. Classification of information.
6. FIPS Publication 199 categorization and level of protection (Low, Moderate, or High).

(Continued)

(Continued)
INFORMATION ASSET MANAGEMENT **5305.5** (Cont. 1)
(Revised 6/14)

7. Importance of information asset to the execution of the state entity's mission and program function.
8. Potential consequences and impacts if confidentiality, integrity and availability of the information asset were compromised.

Implementation Controls: NIST SP 800-53: Planning (PL); Program Management (PM); Information Security Program Management Standard (SIMM 5305-A); and FIPS Publication 199.

RISK MANAGEMENT **5305.6**
(Revised 6/14)

Policy: Each state entity shall create a state entity-wide information security, privacy and risk management strategy which includes a clear expression of risk tolerance for the organization, acceptable risk assessment methodologies, risk mitigation strategies, and a process for consistently evaluating risk across the organization with respect to the state entity's risk tolerance, and approaches for monitoring risk over time.

The state entity's risk management strategy and methodologies shall be consistent with NIST SP 800-30 and NIST SP 800-39, and must include:

1. Risk assessments conducted at the three various levels of the risk management hierarchy, including:
    a. Organizational level;
    b. Mission/Business process level; and
    c. Information asset level.
2. A risk assessment process to identify and assess risks associated with its information assets and define a cost-effective approach to managing such risks; including, but not limited to:
    a. Risk associated with introducing new information processes, systems and technology into the state entity environment;
    b. Accidental and deliberate acts on the part of state entity personnel and outsiders;
    c. Fire, flooding, and electric disturbances; and,
    d. Loss or disruption of data communications capabilities.

Implementation Controls: NIST SP 800-53: Planning (PL); Program Management (PM); and SIMM 5305-A

RISK ASSESSMENT **5305.7**
(Revised 6/14)

Policy: Each state entity shall conduct 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/asset and the information it processes, stores, or transmits. Each state entity shall conduct a comprehensive risk assessment once every two years which assesses the state entity's risk management strategy for all three levels and documents the risk assessment results in a risk assessment report.

The risk assessment process must include the following:

1. Assignment of responsibilities for risk assessment, including appropriate participation of executive, technical, and program management.
2. Identification of the state entity information assets that are at risk, with particular emphasis on the applications of information technology that are critical to state entity program operations. Identification of the threats to which the information assets could be exposed.
3. Assessment of the vulnerabilities, e.g., the points where information assets lack sufficient protection from identified threats.
4. Determination of the probable loss or consequences, based upon quantitative and qualitative evaluation, of a realized threat for each vulnerability and estimation of the likelihood of such occurrence.
5. Identification and estimation of the cost of protective measures which would eliminate or reduce the vulnerabilities to an acceptable level.
6. Selection of cost-effective security management measures to be implemented.
7. Preparation of a report, to be submitted to the state entity head and to be kept on file within the state entity, documenting the risk assessment, the proposed security management measures, the resources necessary for security management, and the amount of residual risk to be accepted by the state entity.

Implementation Controls: NIST SP 800-53: Risk Assessment (RA)

PROVISIONS FOR AGREEMENTS WITH STATE AND NON-STATE ENTITIES 5305.8

(Revised 6/14)

Introduction: State entities are required to enter into written agreements with state and non-state entities when they engage such entities in the development, use, or maintenance of information systems, products, solutions, or services.

Policy: Each state entity shall ensure agreements with state and non-state entities include provisions which protect and minimize risk to the state. Agreements shall include, at a minimum, provisions which cover the following:

1. Appropriate levels of security (confidentiality, integrity and availability) for the data based on data categorization and classification and FIPS Publication 199 protection levels.
2. Standards for transmission and storage of the data, including encryption and destruction, if applicable.
3. Agreements to comply with statewide policies and laws regarding the use and protection of information resources and data, including those set forth in this Chapter.
4. Signed confidentiality statements.
5. Agreements to apply security patches and upgrades, and keep virus software up-to-date on all systems on which data may be used.
6. Agreements to notify the state data owners promptly if a security incident involving the information system or data occurs.
7. Agreements that the data owner shall have the right to participate in the investigation of a security incident involving its data or conduct its own independent investigation, and that data custodian shall cooperate fully in such investigations.

(Continued)

(Continued)
PROVISIONS FOR AGREEMENTS WITH STATE AND NON-STATE ENTITIES **5305.8** (Cont. 1)
(Revised 6/14)

8. Agreements that the data custodian shall be responsible for all costs incurred by the data owner due to security incident resulting from the data custodian's failure to perform or negligent acts of its personnel, and resulting in an unauthorized disclosure, release, access, review, or destruction; or loss, theft or misuse of an information asset. If the contractor experiences a loss or breach of data, the contractor shall immediately report the loss or breach to the data owner. If the data owner determines that notice to the individuals whose data has been lost or breached is appropriate, the contractor will bear any and all costs associated with the notice or any mitigation selected by the data owner. These costs include, but are not limited to, staff time, material costs, postage, media announcements, and other identifiable costs associated with the breach or loss of data.
9. Agreements that the data custodian shall immediately notify and work cooperatively with the data owner to respond timely and correctly to public records act requests.
10. Agreements between the data custodian and data owner to address the appropriate disposition of records held by the data custodian during the term of its agreement with the data owner.

Implementation Controls: NIST SP 800-53, System and Services Acquisition (SA)

INFORMATION SECURITY PROGRAM METRICS **5305.9**
(Revised 6/14)

Introduction: Performance with respect to security controls must be measured to determine whether the needs of the state entity are being met. Security metrics assist with adjustments to security controls in order to improve effectiveness.

Policy: Each state entity shall establish outcome-based metrics to measure the effectiveness and efficiency of the state entity's information security program, and the security controls deployed.

Implementation Controls: NIST SP 800-53: System and Services Acquisition (SA); Security Assessment and Authorization (CA); Contingency Planning (CP)

PRIVACY **5310**
(Revised 6/14)

Introduction: Privacy can be understood as the rights of individuals, as defined by law, to control the collection and use of their personal information. This privacy policy is based generally on the Information Practices Act of 1977 (Civil Code section 1798, et seq.). In addition to its general application, the Information Practices Act of 1977 is broad in scope, drawing from the Fair Information Practice Principles (FIPPs), which form the basis for most privacy laws in the United States and around the world. The FIPPs help entities attain public trust and mitigate loss and risk stemming from privacy incidents.

Included among the principles are transparency, notice, and choice. Some state entities are also subject to additional state and federal privacy laws related to particular types of personal information.

Governing Authority: The following overarching privacy laws are applicable to state entities:

1. Article 1, Section 1, of the Constitution of the State of California defines pursuing and obtaining privacy as an inalienable right.

2. The Information Practices Act of 1977 (Civil Code section 1798, et seq.) places specific requirements on each state entity in the collection, use, maintenance, and dissemination of information relating to individuals.

3. Government Code Section 11019.9 requires state agencies to enact and to maintain a privacy policy and to designate an employee to be responsible for the policy. The policy must describe the agency's practices for handling personal information, as further required in the Information Practices Act.

Policy: State entity heads shall direct the establishment of an entity-specific Privacy Program. The Privacy Program shall ensure, and privacy coordinators shall confirm, that the requirements contained in the California Information Practices Act, this policy and the associated standards are adhered to by the state entity and its personnel.

Implementation Controls: NIST SP 800-53: Appendix J-Privacy Control Catalog

STATE ENTITY PRIVACY STATEMENT AND NOTICE ON COLLECTION 5310.1

(Revised 6/14)

Policy: Information asset owners shall be open about state entity information handling practices, including the purposes for which the state entity collects, uses, and discloses personal information of individuals. Each state entity Privacy Program Coordinator shall prepare, publish, and maintain a General Privacy Policy Statement and a Privacy Notice on Collection for each personal information collection in accordance with the Privacy Statement and Notices Standard (SIMM 5310-A).

General Privacy Policy Statement
Each state entity's general privacy policy, as required by Government Code section 11019.9, shall apply to the entire state entity and its subdivisions.

Privacy Notice on Collection
When personal information is collected from an individual on or with any form, the information asset owner shall ensure that notice is provided to the individual at or before the time of collection. The content and presentation of the notice shall comply with requirements outlined in the Privacy Statement and Notices Standard (SIMM 5310-A).

Implementation Controls: NIST SP 800-53: Appendix J-Privacy Control Catalog, and SIMM 5310-A

LIMITING COLLECTION 5310.2

(Revised 6/14)

Policy: Information asset owners shall collect the least amount of personal information that is required to fulfill the purposes for which it is being collected. Information asset owners shall obtain personal information only through lawful means and shall collect personal information to the greatest extent practicable directly from the individual who is the subject of the information rather than from another source. Information asset owners shall endeavor to collect non-personal information, instead of personal information, if it is able to fulfill the same requirements.

Implementation Controls: NIST SP 800-53: Appendix J-Privacy Control Catalog

LIMITING USE AND DISCLOSURE 5310.3

(Revised 6/14)

Policy: Information asset owners, custodians and users shall not disclose, use, or make available personal information collected from individuals for purposes other than those for which it was originally collected, except in the following situations:

1. The disclosure is made to the individual who is the subject of the information;
2. The nature of the disclosure is included in the Privacy Notice on Collection provided at or before the time of collection;
3. The individual who is the subject of the information, subsequent to collection, provides explicit consent to the disclosure or use; or
4. The use or disclosure is explicitly allowed under Civil Code section 1798.24.

Accounting of Disclosures

Information asset owners shall keep an accurate accounting of the date, nature, and purpose of each disclosure of a record made under exception number 4 above. The accounting shall include the date of the disclosure, and the name, title, and business address of the individual or state entity to which the disclosure was made.

Information asset owners shall retain the above referenced accounting for at least three years after the disclosure for which the accounting is made, or until the record is destroyed in accordance with the state entity record retention policy, whichever is shorter.

Information asset owners shall inform any individual or state entity to whom a record containing personal information has been disclosed during the preceding three years of any correction of an error in the record or notation of a dispute about its accuracy.

Use of Information by Third Parties

Information asset owners and users shall apply the requirements of this policy to any third party who handles personal information collected by the state entity, in order to accomplish a state entity function that is consistent with the original purposes for which it was collected. Any such third party and its personnel or agent with access to the personal information shall formally agree to be subject to the state entity's privacy policies and practices in the same manner as an employee of the state entity.

(Continued)

(Continued)
LIMITING USE AND DISCLOSURE **5310.3 (Cont. 1)**
(Revised 6/14)

Social Security Numbers
Information asset owners shall minimize the collection and use of Social Security numbers. Information asset owners shall not publicly post or publicly display in any manner an individual's Social Security number or otherwise permit handling of Social Security numbers in any manner inconsistent with the Privacy Individual Access Standard (SIMM 5310-B).

Information asset owners shall not permit Social Security numbers to be either entered into systems as authentication credentials or used as user unique identifiers within systems. This requirement shall apply to all new systems, and major changes or upgrades to existing systems.

Implementation Controls: NIST SP 800-53: Appendix J-Privacy Control Catalog, and SIMM 5310-B

INDIVIDUAL ACCESS TO PERSONAL INFORMATION 5310.4

(Revised 6/14)

Policy: Each state entity shall ensure individuals are provided with information about their access rights and the procedures for exercising those rights.

Individuals Right to Access

Each state entity Privacy Program Coordinator shall publish procedures for individuals to follow in exercising their rights to access records held by the state entity which contain their personal information. Such rights include the right to inquire and be informed as to whether the state entity maintains a record about the individual and the right to request a correction of or an amendment to their personal information. Such procedures shall be made available online if the state entity has a website, and shall otherwise comply with the Privacy Individual Access Standard (SIMM 5310-B).

Personal Information in Public Records

Each state entity head shall include in the state entity's procedures for access to public records, a provision requiring the redaction of personal information prior to allowing inspection or releasing records in response to a California Public Records Act request.

Mailing Lists

Upon written request of an individual, an information asset owner maintaining a mailing list shall remove the individual's name and contact information from such list, unless such name and contact information is exclusively used by the state entity to directly contact the individual. Information asset owners shall inform individuals, in the requisite Privacy Notice on Collection forms used to collect personal information, of their right to have their information removed from such mailing lists.

Implementation Controls: NIST SP 800-53: Appendix J-Privacy Control Catalog , and SIMM 5310-B

INFORMATION INTEGRITY **5310.5**
(Revised 6/14)

Policy: Information asset owners shall maintain all records with accuracy, relevance, timeliness, and completeness.

Maintaining Record Integrity
When an information asset owner uses a record to make a determination about an individual or transfers a record to another state or non-state entity, the owner shall correct, update, withhold, or delete any portion of the record that it knows or has reason to believe is inaccurate or out of date.

Maintaining Information Sources
Whenever an information asset owner collects personal information, the owner shall either ensure that the individual is provided a copy of the source document or shall record and maintain the source of the information, unless the source is the individual record subject.

Ownership of Stored Records and State Archived Records

1. Stored Records: When records that contain personal information are transferred to the Department of General Services (DGS) for storage, information asset owners for the state entity transferring the records shall retain all owner responsibilities for the protection of the record as provided in this Chapter. The DGS shall not disclose the record except to the information asset owner or his designee, or in accordance with their instructions which must be in accordance with this policy and relevant laws.
2. State Archives: Information asset owners shall transfer a record pertaining to an identifiable individual to the State Archives only after determining, with concurrence by the state entity head, that the record has sufficient historical or other value to warrant its continued preservation by the California state government. In the event of this transfer, information asset ownership shall be formally transferred to an information asset owner in the State Archives, who shall accept all owner responsibilities contained in the enterprise information security and privacy policies and standards.

Implementation Controls: NIST SP 800-53: Appendix J-Privacy Control Catalog

DATA RETENTION AND DESTRUCTION 5310.6

(Revised 6/14)

Policy: Information asset owners shall retain and/or destroy records of personal information in accordance with the state entity's record retention and destruction policy and the Privacy Individual Access Standard (SIMM 5310-B). Information asset owners shall take reasonable steps to keep personal information only as long as is necessary to carry out the purposes for which the information was collected.

However, no record of personal information shall be destroyed or otherwise disposed of by any state entity unless:

a. It is determined by the state entity head that the record has no further administrative, legal, or fiscal value;
b. The state entity head has determined that an audit has been performed for any record subject to audit; and
c. The Secretary of State has determined that the record is inappropriate for preservation in the State Archives.

Destruction of Electronically Collected Personal Information
An information asset owner shall, upon request by the record subject, securely discard without reuse or distribution, any personal information collected through a state entity's website.

Implementation Controls: NIST SP 800-53: Appendix J-Privacy Control Catalog, and SIMM 5310-B

SECURITY SAFEGUARDS 5310.7

(Revised 6/14)

Policy: Information asset owners shall apply all applicable statewide and state entity information security laws, policies, standards, and procedures in order to protect personal information under the information asset owner's responsibility.

Implementation Controls: NIST SP 800-53: Appendix J-Privacy Control Catalog

INFORMATION SECURITY INTEGRATION 5315

(Revised 6/14)

Policy: Each state entity is responsible for the integration of information security and privacy within the organization. This includes, but is not limited to, the designing of appropriate security controls in new systems, or systems that are undergoing substantial redesign, including both in-house and outsourced solutions. Each state entity shall ensure its ISO, and where applicable its Privacy Program Coordinator and Technology Recovery Coordinator, are actively engaged with the owners of information, and project, procurement and technical personnel involved with information asset acquisition, development, operations, maintenance and disposal to:

1. Ensure information security is considered throughout the asset lifecycle, from acquisition and development through maintenance and operations, to retirement.
2. Integrate information security design requirements into both manual information handling and information processing functions, and information technology activities, including throughout the system development lifecycle (SDLC);
3. Create system security plans outlining key information security controls to mitigate risks;
4. Create and maintain residual risk documentation consistent with the State Information Management Principles, Record of Decisions (SAM Section 4800);
5. Integrate information security (confidentiality, integrity, and availability) requirements into contracts for outsourced products and services, and any agreements with state and non-state entities;
6. Create, maintain, and enforce information security policies, standards, procedures, and guidelines;
7. Create secure configuration standards for hardware, software, and network devices; and
8. Implement administrative, technical, and physical controls for the protection of information assets as part of the system engineering process.

Implementation Controls: NIST SP 800-53: System and Services Acquisition (SA)

SYSTEM AND SERVICES ACQUISITION 5315.1

(Revised 6/14)

Policy: Each state entity shall determine the information security requirements (confidentiality, integrity, and availability) for its information assets in mission/business process planning; determine, document and allocate the resources required to protect the information assets as part of its capital planning and investment control process; and, establish organizational programming and budgeting documentation.

For all information system acquisitions, the state entity shall identify security functional, strength and assurance requirements; security-related documentation requirements; a description of the information system development and intended operational environments; and acceptance criteria.

Implementation Controls: NIST SP 800-53: System and Services Acquisition (SA)

SYSTEM DEVELOPMENT LIFECYCLE 5315.2

(Revised 6/14)

Policy: Each state entity shall manage its information assets using a documented SDLC methodology that:

1. Incorporates information security requirements and considerations;
2. Defines and documents operational information security roles and responsibilities throughout the information asset lifecycle;
3. Identifies individuals having information security roles and responsibilities; and
4. Integrates the organizational information security risk management process into the development lifecycle activities.

Implementation Controls: NIST SP 800-53: System and Services Acquisition (SA)

INFORMATION ASSET DOCUMENTATION 5315.3

(Revised 6/14)

Policy: In conjunction with Records Management (SAM Chapter 1600) and Property Accounting (SAM Chapter 8600) requirements, each state entity shall ensure information security documentation is prepared and maintained as part of the overall documentation for all information assets. Documentation shall include a description of the effective use and maintenance of security controls and the state entity's responsibilities in maintaining the security of the information assets. Each state entity shall obtain administrator and user documentation for each information system, and provisions for the protection of documentation from loss, theft, damage, or misuse.

Implementation Controls: NIST SP 800-53: System and Services Acquisition (SA); SAM Chapters 1600 and 8600

SYSTEM DEVELOPER SECURITY TESTING **5315.4**
(Revised 6/14)

Policy: Each state entity shall require that system developers create and implement a security test and evaluation plan as part of the system design and build. When a contract is required, it shall specify the acceptance criteria for security test and evaluation plans and vulnerability remediation processes.

Implementation Controls: NIST SP 800-53: System and Services Acquisition (SA)

CONFIGURATION MANAGEMENT **5315.5**
(Revised 6/14)

Policy: Each state entity shall establish a documented process regarding controlled modifications to hardware, firmware, and software to protect the information asset against improper modification before, during, and after system implementation.

Implementation Controls: NIST SP 800-53: Configuration Management (CM)

ACTIVATE ONLY ESSENTIAL FUNCTIONALITY **5315.6**
(Revised 6/14)

Policy: Each state entity shall configure information assets to provide only essential capabilities and functionality, and shall adhere to the principle of least privilege and restrict the use of unnecessary ports, protocols, and/or services to minimize the state entity's risk.

Implementation Controls: NIST SP 800-53: Configuration Management (CM)

SOFTWARE USAGE RESTRICTIONS **5315.7**
(Revised 6/14)

Policy: Each state entity shall ensure its Software Management Plan (SAM sections 4846.1 and 4846.2) addresses the following:

1. Use of software and associated documentation in accordance with contract agreements and copyright laws;
2. Enforcement of explicit rules governing the authorized installation of software by users; and
3. Maintaining control over the types of software installed by identifying permitted and prohibited software installations.

Implementation Controls: NIST SP 800-53: Configuration Management (CM)

INFORMATION ASSET CONNECTIONS 5315.8

(Revised 6/14)

Policy: Each state entity shall carefully consider the risks that may be introduced when information assets are connected to other systems with different security requirements and security controls, both within the state entity and external to the state entity.

Each state entity shall identify and maintain an inventory of its authorized information system connections with other state entities which establish authorized connections from information assets as defined by their authorization boundary, to other information systems. Each state entity shall document, for each connection, the interface characteristics, security requirements, the nature of the information communicated, and ensure written agreements are established and maintained which include the minimum provisions for agreements with state and non-state entities as outlined in SAM Section 5305.8.

This policy applies to dedicated connections between information assets and does not apply to transitory, user-controlled connections such as email and website browsing.

Implementation Controls: NIST SP 800-53: Access Control (AC)

SECURITY AUTHORIZATION 5315.9

(Revised 12/13)

Introduction: The authorizing official(s) provide budgetary oversight for state entity information assets and assume responsibility for the mission/business operations supported by those systems.

Policy: Consistent with the State Information Management Principles, Record of Decisions (SAM section 4800), each state entity shall establish a documented security authorization method which tracks official management decisions authorizing the operation of information assets and explicit acceptance of risks based on implementation of agreed-upon information security measures. The state entity head shall assign senior-level executive(s) or manager(s) as the authorizing official(s).

TRAINING AND AWARENESS FOR INFORMATION SECURITY AND PRIVACY 5320

(Revised 6/14)

Policy: Each state entity must establish and maintain an information security and privacy training and awareness program. State entity personnel must possess the knowledge and skills necessary to use information technology to the best advantage for the state. Each state entity must regularly assess the skills and knowledge of its personnel in relation to job requirements, identify and document training and professional development needs, and provide suitable training within the limits of available resources.

The training and awareness program shall ensure:

1. All personnel receive general security and privacy awareness training so that they understand the state entity information security policies, standards, procedures, and practices; and are knowledgeable about the various management, operational, and technical controls required to protect the information assets for which they are responsible.
2. Groups of personnel with special security training needs, such as application developers receive the necessary training.
3. Training records are maintained to support corrective action, audit and assessment processes.
4. The program content is maintained and evaluated for effectiveness on an ongoing basis.

State entity heads, Chief Information Officers (CIOs), ISOs, management, and information asset owners have key roles in information security training and awareness. The state entity head is responsible for ensuring an effective program is implemented state entity-wide. The scope and content of the awareness program must align with statewide policy, and with any state entity specific security needs and requirements.

Implementation Controls: NIST SP 800-53: Awareness and Training (AT)

SECURITY AND PRIVACY AWARENESS 5320.1

(Revised 12/13)

Policy: Each state entity shall provide basic security and privacy awareness training to all information asset users (all personnel, including managers and senior executives) as part of initial training for new users and annually thereafter.

Each state entity shall determine the appropriate content of security awareness training based on statewide requirements, specific state entity requirements, and the information processes and assets to which personnel have access.

SECURITY AND PRIVACY TRAINING 5320.2

(Revised 6/14)

Policy: Each state entity shall determine the appropriate content of security and privacy training based on the assigned roles and responsibilities of individuals and the specific security requirements of the state entity and the information assets to which personnel have access. Privacy training content will ensure personnel understand their responsibility for compliance with the Information Practices Act of 1977 and the penalties for non-compliance.

Governing Provisions: Civil Code section 1798

Implementation Controls: NIST SP 800-53: Awareness and Training (AT)

SECURITY AND PRIVACY TRAINING RECORDS **5320.3**
(Revised 6/14)

Policy: Each state entity shall document and monitor individual information security and privacy training activities including basic security and privacy awareness training and specific information system security training; and retain individual training records to support corrective action, audit and assessment processes. The ISO will be responsible for ensuring that training content is maintained and updated as necessary to address the latest security challenges that may impact users.

Implementation Controls: NIST SP 800-53: Awareness and Training (AT)

PERSONNEL SECURITY **5320.4**
(Revised 6/14)

Policy: Each state entity shall establish processes and procedures to ensure that individual access to information assets is commensurate with job-related responsibilities, and individuals requiring access to information assets sign appropriate user agreements prior to being granted access.

Access agreements shall include acceptable use provisions, and may also include nondisclosure agreements and conflict-of-interest agreements. If required by law, regulation or policy, each state entity must ensure individuals obtain applicable security clearances.

Personnel transfers or reassignments to other positions within the state entity must be reviewed to prevent accumulation of access and support least access privilege. Returning and issuing keys, identification cards, and building passes; closing information system accounts and establishing new accounts; and changing information system access authorizations are all examples of personnel security practices related to staff transfer or reassignment.

Implementation Controls: NIST SP 800-53: Personnel Security (PS)

BUSINESS CONTINUITY WITH TECHNOLOGY RECOVERY 5325

(Revised 6/14)

Introduction: The entire concept of business continuity is based on the identification of all business functions within a state entity, and then assigning a level of importance to each business function. A business impact assessment is the primary tool for gathering this information and assigning criticality, recovery point objectives, and recovery time objectives, and is therefore part of the basic foundation of contingency planning and business continuity.

Policy: Each state entity shall ensure individuals with knowledge about business functions of the organization lead and participate in the business continuity planning process to:

1. Identify and document all business functions;
2. Conduct a business impact assessment to identify:
    a. critical functions and systems, and prioritize them based on necessity;
    b. threats and vulnerabilities; and
    c. preventive controls and countermeasures to reduce the state entity's risk level.
3. Develop recovery strategies to ensure systems and functions can be brought online quickly;
4. Develop the Business Continuity Plan to include procedures for how the state entity will stay functional in a disastrous state;
5. Conduct regular training to prepare individuals on their expected tasks;
6. Conduct regular tests and exercises to identify any deficiencies and further refine the plan; and
7. Develop steps to ensure the Business Continuity Plan is maintained and updated regularly.

Note: The Business Continuity Plan must also address the Office of Emergency Services' continuity planning requirements. These are available at: http://www.caloes.ca.gov/cal-oes-divisions/planning-preparedness/continuity-planning

Implementation Controls: NIST SP 800-34; NIST SP 800-53: Contingency Planning (CP)

TECHNOLOGY RECOVERY PLAN 5325.1

(Revised 6/14)

Introduction: The Technology Recovery Plan (TRP) is a sub-set of the state entity's Business Continuity Plan. The TRP is activated immediately after a disaster strikes and focuses on getting critical systems back online.

Policy: Each state entity shall develop a TRP in support of the state entity's Continuity Plan and the business need to protect critical information assets to ensure their availability following an interruption or disaster. Each state entity must keep its TRP up-to-date and provide annual documentation for those updates to the CISO. The annual requirements are:

1. Each state entity must file a copy of its TRP and the Technology Recovery Program Compliance Certification (SIMM 5325-B) with the CISO, in accordance with the Technology Recovery Plan Submission Schedule.
2. If the state entity employs the services of a data center it must work with the data center to establish and document TRP coordination procedures.

   Each state entity TRP must cover, at a minimum, the program areas which are listed and described in the Technology Recovery Plan Documentation for Agencies Preparation Instructions (SIMM 5325-A). If the TRP does not follow the format in SIMM 5325-A, a cross reference sheet, SIMM 5325-B, must be included with the update to indicate where required information is located.

The TRP must outline a planned approach to managing risks to the state entity's mission, including risk and potential impact to critical information technology assets. The TRP must be derived from the state entity's business impact assessment and Business Continuity Plan. Instructions for preparing the TRP are described in SIMM 5325-A.

Implementation Controls: NIST SP 800-34; NIST SP 800-53: Contingency Planning (CP)

TECHNOLOGY RECOVERY TRAINING 5325.2

(Revised 6/14)

Policy: Each state entity shall establish technology recovery training and exercises for personnel involved in technology recovery, to ensure availability of skilled staff. The training exercises shall include a crisis communication plan, event status reporting requirements, and focused role-based training for managers and system administrators.

Implementation Controls: NIST SP 800-53: Contingency Planning (CP)

TECHNOLOGY RECOVERY TESTING **5325.3**
(Revised 6/14)

Policy: Each state entity shall test the TRP to determine its effectiveness and the state entity's readiness to execute the TRP in the event of a disaster. Each state entity shall initiate corrective actions and improvements to the TRP based upon deficiencies identified during testing and exercises.

Implementation Controls: NIST SP 800-53: Contingency Planning (CP)

ALTERNATE STORAGE AND PROCESSING SITE **5325.4**
(Revised 6/14)

Policy: Each state entity shall establish an alternate storage site, including the necessary agreements to permit the storage and recovery of backup information. Each state entity shall ensure that the alternate storage site provides information security safeguards equivalent to that of the primary site.

Implementation Controls: NIST SP 800-53: Contingency Planning (CP)

TELECOMMUNICATIONS SERVICES **5325.5**
(Revised 6/14)

Policy: Each state entity shall ensure they have alternate telecommunications services including necessary agreements to permit the resumption of information asset operations for essential missions and business functions when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

Implementation Controls: NIST SP 800-53: Contingency Planning (CP)

INFORMATION SYSTEM BACKUPS **5325.6**
(Revised 6/14)

Policy: Each state entity shall perform regularly scheduled backups of system and user-level information. Backups shall be:

1. Conducted at the operating system, application, and user level;
2. Conducted of information system documentation including security-related documentation;
3. Stored in a protected locations; and
4. Securely destroyed upon expiration of retention period.

System-level information includes system-state information, operating system and application software, and software licenses. User-level information includes any information other than system-level information. Mechanisms to protect the integrity of information system backups shall include digital signatures and cryptographic hashes. Information system backups shall reflect the requirements in contingency plans as well as other state entity requirements for backing up information.

Implementation Controls: NIST SP 800-53: Contingency Planning (CP)

INFORMATION SECURITY COMPLIANCE **5330**
(Revised 6/14)

Policy: Each state entity shall validate compliance with statewide information security policy, standards, and procedures as set forth in this Chapter, and the state entity's internal information security policies to verify that security measures are in place and functioning as intended. Each state entity's validation processes shall include:

1. Ongoing assessments of key security measures and controls in both in-house and outsourced systems;
2. Completion of independent "pre-production" assessments of security controls in new systems or systems that are undergoing substantial redesign;
3. Adherence to the CISO reporting requirements;
4. Coordination of all IT audit and assessment work done by third-party auditors; and
5. Monitoring of third-party auditors' compliance to statewide information security requirements as set forth in this Chapter.

Implementation Controls: NIST SP 800-53: Security Assessment and Authorization (CA)

SECURITY ASSESSMENTS **5330.1**
(Revised 6/14)

Policy: Each state entity shall perform security assessments to determine whether the security controls selected by the state entity are implemented correctly and working as intended to mitigate risk. Security assessments conducted by the state entity shall include, but are not limited to, the following:

1. Legal, policy, standards, and procedure compliance review;
2. Vulnerability scanning; and
3. Penetration testing.

Implementation Controls: NIST SP 800-53: Security Assessment and Authorization (CA)

COMPLIANCE REPORTING **5330.2**
(Revised 12/13)

Policy: Each state entity shall comply with the following reporting requirements as directed by the CISO:

1. Designation Letter – By January 31 of each year, and as designee changes occur, the state entity head shall designate an ISO, Technology Recovery Coordinator and Privacy Officer/Coordinator using the Designation Letter (SIMM 5330-A). Upon the designation of a new ISO, Disaster Recovery Coordinator, and/or Privacy Program Coordinator, the state entity must submit an updated Designation Letter to the CISO within ten (10) business days using the Designation Letter (SIMM 5330-A).
2. Risk Management and Privacy Program Compliance Certification – By January 31 of each year, the state entity head shall certify that the entity is in compliance with state policy governing information security, risk management and privacy program compliance by submitting the Risk Management and Privacy Program Compliance Certification (SIMM 5330-B).
3. Technology Recovery Plan – Each year the state entity head shall submit a copy of its Technology Recovery Plan (TRP) with the Technology Recovery Program Compliance Certification (SIMM 5325-B) to the CISO by the due date outlined in the Technology Recovery Plan Submission Schedule. If the state entity employs the services of a data center, it must also provide the data center with a copy of its TRP or subset of the relevant recovery information from the state entity's TRP.
4. Incident Follow-up Report – Within ten (10) business days from the date of reporting an incident, each state entity must complete an Information Security Incident Report (SIMM 5340-B). The CISO may require, in conjunction with its assessment of the incident, that the state entity provide additional information.

INFORMATION SECURITY MONITORING 5335

(Revised 6/14)

Policy: Each state entity is responsible for continuous monitoring of its networks and other information assets for signs of attack, anomalies, and suspicious or inappropriate activities.

Each state entity shall ensure:

1. An event logging and monitoring strategy which provides for audit trails and auditability of events and appropriate segregation and separation of duties;
2. Event logging and log monitoring are performed with sufficient regularity that signs of attack, anomalies, and suspicious or inappropriate activities are identified and acted upon in a timely manner;
3. Sensors, agents, and security monitoring software are placed at strategic locations throughout the network;
4. Situational awareness information from security monitoring and event correlation tools are monitored to identify events that require investigation and response; and
5. Potential security events are reported immediately to the security incident response team.

Implementation Controls: NIST SP 800-53: Audit and Accountability (AU); Physical and Environmental Protection (PE); Risk Assessment (RA)

CONTINUOUS MONITORING 5335.1

(Revised 6/14)

Introduction: Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support state entity risk management decisions.

Policy: Each state entity shall develop a continuous monitoring strategy and implement a continuous monitoring program.

Implementation Controls: NIST SP 800-53: Audit and Accountability (AU); Physical and Environmental Protection (PE); Risk Assessment (RA); Security Assessment and Authorization (CA)

AUDITABLE EVENTS **5335.2**
(Revised 6/14)

Introduction: Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the right level of abstraction is a critical aspect of an audit capability and can facilitate the identification of root causes to events. Each state entity 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 extreme burden on system performance.

Policy: Each state entity shall ensure that information systems are capable of being audited and the events necessary to reconstruct transactions and support after-the-fact investigations are maintained. This includes the auditing necessary to cover related events, such as the various steps in distributed, transaction-based processes (e.g., processes that are distributed across multiple organizations) and actions in service-oriented architectures.

Implementation Controls: NIST SP 800-53: Audit and Accountability (AU); Physical and Environmental Protection (PE); Risk Assessment (RA)

INFORMATION SECURITY INCIDENT MANAGEMENT 5340

(Revised 6/14)

Policy: Each state entity must promptly investigate incidents involving loss, theft, damage, misuse of information assets, or improper dissemination of information. All state entities are required to report information security incidents consistent with the security reporting requirements in this policy and manage information security incidents to determine the cause, scope, and impact of incidents to stop unwanted activity, limit loss and damage, and prevent recurrence. Additionally, each state entity shall develop, disseminate, and maintain a formal, documented incident response plan that provides for the timely assembly of appropriate staff that is capable of developing a response to, appropriate reporting about, and successful recovery from a variety of incidents.

Each state entity shall develop documented procedures to facilitate the implementation of the incident response plan and associated incident response controls including, but are not limited to:

1. Immediately reporting suspected and actual security incidents in accordance with the criteria and procedures set forth in SIMM 5340-A and other applicable laws and regulations;
2. Managing security incident case assignments and the security investigation process in a timely and effective manner;
3. Managing security incidents involving a breach of personal information in accordance with the criteria and procedures set forth in SIMM 5340-C.
4. Mobilizing emergency and third party investigation and response processes if necessary;
5. Consulting with system owners to help quarantine incidents and limit damage;
6. Consulting with Personnel Management if there is a violation of appropriate use policy; and
7. Communicating with law enforcement when actual or suspected criminal activity is involved.

Implementation Controls: NIST SP 800-53: Incident Response (IR); SIMM 5340-A; SIMM 5340-C

INCIDENT RESPONSE TRAINING 5340.1

(Revised 6/14)

Policy: Each state entity shall provide incident response training to information system users consistent with assigned roles and responsibilities.

Incident response training shall be at an appropriate level for the assigned roles and responsibilities of state entity personnel. For example, regular users may only need to know who to call or how to recognize an incident; system administrators may require additional training on how to handle/remediate incidents; and incident responders may need more specific training on chain of custody, forensics, reporting, system recovery, and restoration. Incident response training shall include, at a minimum, user training in the identification and reporting of suspicious activities, both from external and internal sources.

Implementation Controls: NIST SP 800-53: Incident Response (IR)

INCIDENT RESPONSE TESTING 5340.2

(Revised 6/14)

Introduction: Incident response testing includes an assessment of the effects on state entity operations (e.g., reduction in mission capabilities), state entity assets, and individuals due to incident response, and involves the use of checklists, walk-through or tabletop exercises, and simulations to prepare personnel and mitigate the impacts of actual incidents.

Policy: Each state entity shall exercise or test their incident response capability to determine its effectiveness, document the results and incorporate lessons learned to continually improve the plan.

Implementation Controls: NIST SP 800-53: Incident Response (IR)

INCIDENT HANDLING 5340.3

(Revised 6/14)

Policy: Each state entity shall implement incident handling for information security and privacy incidents that includes preparation, detection and analysis, containment, eradication, and recovery. Incident handling shall coordinate with business continuity planning activities (SAM section 5325). Incident handling capability shall include procedures for coordination among many groups within a state entity, 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 executive management.

Implementation Controls: NIST SP 800-53: Incident Response (IR)

INCIDENT REPORTING 5340.4

(Revised 6/14)

Policy: Each state entity shall follow the incident reporting procedures as described in SIMM 5340-A.

Implementation Controls: NIST SP 800-53: Incident Response (IR); SIMM 5340-A

VULNERABILITY AND THREAT MANAGEMENT 5345

(Revised 6/14)

Introduction: Threats and vulnerabilities provide the primary inputs to the state entity's risk assessment process.

Policy: Each state entity shall continuously identify and remediate vulnerabilities before they can be exploited. Vulnerability and threat management include, but not limited to, the following:

1. Strategic placement of scanning tools to continuously assess all information technology assets;
2. Implementation of appropriate scan schedules, based on asset criticality;
3. Communication of vulnerability information to system owners or other individuals responsible for remediation;
4. Dissemination of timely threat advisories to system owners or other individuals responsible for remediation; and
5. Consultation with system owners on mitigation strategies.
6. Implementation of mitigation measures.

Implementation Controls: NIST SP 800-53: Risk Assessment (RA); System and Services Acquisition (SA); System and Communication Protection (SC)

OPERATIONAL SECURITY 5350

(Revised 6/14)

Introduction: In order to mitigate against successful attacks, each state entity is responsible for separating and controlling access to various systems and networks with different threat levels and sets of users which may operate or interface within their technology environment.

Policy: Each state entity shall develop, implement, and document, disseminate, and maintain operational security practices which include, but are not limited to:

1. A network security architecture that:
    a. includes distinct zones to separate internal, external, and DMZ traffic; and
    b. segments internal networks to limit damage, should a security incident occur.
2. Firewall, router, and other perimeter security tools which enforce network security architecture decisions.
3. Periodic review of perimeter security access control rules to identify those that are no longer needed or provide overly broad access.

Each state entity's security architecture shall align with the following security controls and best practices:

1. Application partitioning;
2. Denial of service protection;
3. Boundary protection;
4. Confidentiality of transmitted information or appropriate compensating security controls if protection assurances cannot be guaranteed; and
5. Cryptographic protections using modules that comply with FIPS-validated cryptography.

Implementation Controls: NIST SP 800-53: System and Information Integrity (SI); System and Communications Protection (SC)

ENCRYPTION **5350.1**
(Revised 6/14)

Policy: End-to-end encryption or approved compensating security control(s) shall be used to protect confidential, sensitive, or personal information that is transmitted or accessed outside the secure internal network (e.g., email, remote access, file transfer, Internet/website communication tools) of the state entity, or stored on portable electronic storage media (e.g., USB flash drives, tapes, CDs, DVDs, disks, SD cards, portable hard drives), mobile computing devices (e.g., laptops, netbooks, tablets, and smartphones), and other mobile electronic devices. In rare instances where encryption cannot be implemented, compensating control(s) or alternatives to encryption must be in place. Compensating controls and alternatives to encryption must be reviewed on a case-by-case basis and approved in writing by the state entity ISO, after a thorough risk analysis.

Implementation Controls: FIPS 140-2, FIPS 197, NIST SP 800-53: Access Control (AC), and System and Communications Protection Controls (SC)

ENDPOINT DEFENSE **5355**
(Revised 6/14)

Policy: Each state entity shall be responsible for protecting information on computers that routinely interact with untrusted devices on the internet or may be prone to loss or theft.

Each state entity shall develop and implement methods and techniques to manage processes and tools to:

1. Detect malicious software;
2. Permit only trusted software to run on a device, commonly referred to as white listing;
3. Prevent certain software from running on a device, commonly referred to as blacklisting;
4. Identify unauthorized changes to secure configurations; and
5. Encrypt sensitive data.

Implementation Controls: NIST SP 800-53: System and Information Integrity (SI)

MALICIOUS CODE PROTECTION 5355.1

(Revised 6/14)

Policy: Each state entity shall employ malicious code protection mechanisms at information asset entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code.

Malicious code protection mechanisms may not always detect malicious code; therefore, each state entity shall implement additional safeguards to help ensure that software does not perform functions other than those intended. Examples of additional safeguard include, but are not limited to, secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices.

Implementation Controls: NIST SP 800-53: System and Information Integrity (SI)

SECURITY ALERTS, ADVISORIES, AND DIRECTIVES 5355.2

(Revised 6/14)

Policy: Each state entity shall receive information asset security alerts, advisories, and directives from various legitimate external sources and shall act on those to mitigate state entity risk, including generating internal security alerts, advisories, and directives as deemed necessary.

Implementation Controls: NIST SP 800-53: System and Information Integrity (SI)

IDENTITY AND ACCESS MANAGEMENT 5360

(Revised 6/14)

Policy: Each state entity shall safeguard access to information assets by managing the identities of users and devices and controlling access to resources and data bases on a need to know basis throughout the identity lifecycle. Each state entity shall establish processes and procedures to ensure:

1. Maintenance of user identities, including both provisioning and de-provisioning;
2. Enforcement of password policies or more advanced multifactor mechanisms to authenticate users and devices;
3. Management of access control rules, limiting access to the minimum necessary to complete defined responsibilities;
4. Separation of duties to avoid functional conflicts;
5. Periodic recertification of access control rules to identify those that are no longer needed or provide overly broad clearance;
6. Use of privileged accounts that can bypass security are restricted and audited;
7. Systems to administer access based on roles are defined and installed; and
8. Encryption keys and system security certificates are effectively generated, exchanged, stored and safeguarded.

Implementation Controls: NIST SP 800-53: System and Information Integrity (SI)

REMOTE ACCESS 5360.1

(Revised 6/14)

Policy: Each entity shall establish and document allowed methods of remote access to its information systems; establish usage restrictions and implementation guidance for each allowed remote access method; and monitor the information asset for unauthorized remote access. Allowed methods shall comply with the Telework and Remote Access Security Standard (SIMM 5360-A).

Implementation Controls: NIST SP 800-53: Access Control (AC); SIMM 5360-A

WIRELESS ACCESS 5360.2

(Revised 6/14)

Policy: Each state entity shall establish appropriate restrictions and implementation instructions for wireless access, and enforce requirements for wireless connections to information systems. Each state entity shall also proactively search for unauthorized wireless connections including scans for unauthorized Wi-Fi access points.

Implementation Controls: NIST SP 800-53: Access Control (AC); SIMM 5360-A

PHYSICAL SECURITY 5365

(Revised 6/14)

Policy: Each state entity shall establish and implement physical security and environmental protection controls to safeguard information assets against unauthorized access, use, disclosure, disruption, modification, or destruction.
Physical security and environmental controls shall include management and maintenance of:

1. Facility entry controls and badging systems for personnel and visitors;
2. Equipment and media handling/destruction processes;
3. Building emergency procedures;
4. Screening and/or background check processes;
5. Ventilation and temperature control systems; and
6. Fire suppression, water damage prevention, and electrical power fluctuation or failure detection systems.

Each state entity shall issue physical access authorization credentials to state entity personnel and visitors, as appropriate. Personnel with long-term physical access authorization credentials are not considered visitors. Authorization credentials include, but are not limited to, badges, identification cards and smart cards. The strength of authorization credentials necessary, including level of forge-proof badges, smart cards, or identification cards, shall be determined through a risk assessment.

Each state entity shall monitor physical access to information systems to detect and respond to physical security incidents; review physical access logs and, upon occurrence of an incident, coordinate results of reviews and investigations with the state entity incident response capability.

Implementation Controls: NIST SP 800-53: Physical and Environmental Protection (PE)

ACCESS CONTROL FOR OUTPUT DEVICES 5365.1

(Revised 6/14)

Policy: Each state entity shall control access to information system output devices, such as printers and facsimile devices, to prevent unauthorized individuals from obtaining the output.

Implementation Controls: NIST SP 800-53: Physical and Environmental Protection (PE)

MEDIA PROTECTION **5365.2**
(Revised 6/14)

Policy: Each state entity shall safeguard media in digital and/or non-digital form from unauthorized access, use, modification or disposal, inside or outside of the state entity's control areas whether in storage or transport.

Implementation Controls: NIST SP 800-53: Media Protection (MP)

MEDIA DISPOSAL **5365.3**
(Revised 6/14)

Introduction: Sanitization techniques, including clearing, purging, and destruction, prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Sanitization of non-digital media include, but are not limited to, removing a classified appendix from an otherwise unclassified document, deleting meta data or tags embedded in the document properties that may reveal sources of the document, or redacting selected sections or words from a document.

Policy: Each state entity shall sanitize digital and non-digital media prior to disposal or release for reuse, in accordance with applicable standards and policies, including media found in devices such as hard drives, mobile devices, scanners, copiers, and printers.

Implementation Controls: NIST SP 800-53: Media Protection (MP)