5.3.12 Security Analytics and Continuous Monitoring

(a) Introduction and Overview

Information technology environments that support department business functions and services are complex and dynamic computer network environments, which process, manipulate, and store large amounts of data and information. In order to detect unexpected and suspicious activities and events within such complex networks, it is important to continuously monitor computing environments. Continuous monitoring allows the department to rapidly identify anomalous or suspicious activities and events, analyze these events, and respond accordingly.

(b) Objectives

The objective for this policy is to define department requirements for continuous monitoring of department networks and information assets for signs of malicious use, anomalies, and unexpected behavior and usage patterns.

(c) Scope and Applicability

(1) The scope of this policy extends to all State information assets owned or operated by the department, and governs the facilities and information assets owned or operated on behalf of the department by business partners and service providers.

(2) This policy applies to Owners of Information Assets and Information Asset Custodians.

(d) Policy Directives

The department shall ensure that:

(1) A strategy for security analytics and continuous monitoring will be defined, documented, and implemented.

(2) The strategy will be based on security risk management principles in order to determine optimal monitoring locations, methods, and techniques.

(3) The department's security analytics and continuous monitoring strategy will be integrated with the department's security and event logging and monitoring strategy, threat assessments, and security analytics and event correlation.

(4) The department's continuous monitoring is linked to incident response management and other department incident management processes.

(e) Roles and Responsibilities

(1) Department Chief Information Officer (CIO) or Designee:

(A) Owns this policy and is responsible for ensuring that all Owners of Information Assets, Information Asset Custodians, and users of department information assets are aware of this policy and acknowledge their individual responsibilities.

(B) Is responsible for ensuring that this policy is reviewed annually, and updated accordingly.

(C) Is required to audit and assess compliance with this policy at least once every 2 years.

(2) Department Information Security Officer (ISO):

(A) Shall assist Owners of Information Assets and Information Asset Custodians with the implementation of this policy.

(B) Shall assist Owners of Information Assets and Information Asset Custodians in the analysis and assessment of risks posed by anomalous activities or identified events.

(3) Department Owners of Information Assets and Program Management:

(A) In collaboration with the Information Asset Custodians shall ensure that this policy is implemented and implementation is reviewed annually.

(4) Department Information Asset Custodians:

(A) Shall implement technology and process controls.

(B) Shall maintain records of security monitoring controls implemented.

(f) Enforcement

(1) Non-compliance with this policy may result in disciplinary or adverse action as set forth in DOM Chapter 3, Article 22.

(2) The department shall comply with the information security and privacy policies, standards, and procedures issued by the California Department of Technology (CDT), Office of Information Security (OIS). In addition to compliance with the information security and privacy policies, standards, procedures, and filing requirements issued by the OIS, the department 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, ISO, and Privacy Program Officer or Coordinator to identify all security and privacy requirements applicable to their programs and ensure implementation of the requisite controls.

(3) The consequences of negligence and non-compliance with State laws and policies may include department and personal.
(A) Loss of delegated authorities.
(B) Negative audit findings.
(C) Monetary penalties.
(D) Legal actions.

(g) Auditing

(1) The department has the right to audit any activities related to the use of State information assets.
(2) CDT OIS and the department have the statutory right to audit department readiness to respond and recover from an incident.

(h) Reporting

Violations of this policy shall be reported to the department ISO.

(i) Security Variance Process

If compliance is not feasible, or if deviation from this policy is necessary to support a business function, the respective manager shall formally request a security variance as defined by the ISO.

(j) Authority

This policy complies with the State of California Government Code section 11549.3.

(k) Revisions

The CIO or designee shall ensure that the contents of this article are current and accurate.

References

- State Administrative Manual, Section 5335, Information Security Monitoring
- State Administrative Manual, Section 5335.1, Continuous Monitoring
- State Administrative Manual, Section 5335.2, Auditable Events
- National Institute of Standards and Technology, Special Publications 800-53, Audit and Accountability, AU-2, AU-6, AU-7, AU-13
- National Institute of Standards and Technology, Special Publications 800-53, Incident Response, IR-5, IR-10
- National Institute of Standards and Technology, Special Publications 800-53, Physical and Environmental Protection, PE-6
- National Institute of Standards and Technology, Special Publications 800-53, Program Management, PM-9
- National Institute of Standards and Technology, Special Publications 800-53, Risk Assessment, RA-2, RA-3
- National Institute of Standards and Technology, Special Publications 800-53, Security Assessment and Authorization, CA-7
- California Department of Corrections and Rehabilitation, Department Operations Manual, Chapter 3, Article 22
- California Department of Corrections and Rehabilitation, Department Operations Manual,Chapter 4, Article 41, Section 48010.5
- California Government Code, Section 11549.3

Revision History

Effective: 02/2022