State of California

Department of Technology

Information Security Incident Response and Reporting

Statewide Information Management Manual – 5340-A

February 2026

Table of Contents

Revision History

Revision	Date of Release	Owner	Summary of Changes
v.1	August 2012	California Information Security Office (CISO)	Initial release
v.2	September 2013	CISO	SIMM number change, transferred procedural content from State Administrative Manual (SAM), Chapter 5300
v.3	May 2016	CISO	Update incident reporting instructions for SIMM 5340-B: eliminating incident reporting through ENTAC; directing all incident reports to be made through the Cal-CSIRS system
v.4	January 2018	Office of Information Security (OIS)	Office name/address change
v.5	March 2024	OIS	Format update, process update; Expectations of reimaging, ransomware, and reporting to CIO.
v.6	February 2026	OIS	Major update: Revised structure and content to reflect current operations. Consolidated incident reporting into one section and added material on purpose, plan requirements, TRP & Continuity Planning, and incident closure.

Introduction

Purpose

This document outlines the information security Incident response and reporting criteria all State Entities must adhere to in accordance with State Administrative Manual (SAM) 5340, Information Security Incident Management. It has been framed around the National Institute of Standards and Technology (NIST) Cybersecurity Framework, a set of procedures and guidelines for standardizing the addressing of information security and privacy risks within organizations.

Upon discovery of a security Incident, State Entities are to promptly investigate Incidents involving loss, theft, damage, misuse of information assets, or improper dissemination of information. Upon discovery of any Incident that meets the notification and reporting criteria defined herein, all State Entities must immediately report the Incident following the procedures identified in this standard.

Scope

This standard applies to all California State Entities, as defined below.

Compliance

As outlined in Government Code (GC) Section 11549.3, the Office of Information Security (OIS) is entrusted with creating, issuing, and maintaining policies, standards, and procedures, overseeing information security risk management for agencies and State Entities, providing information security and privacy guidance, and ensuring compliance with SAM Chapter 5300 and Statewide Information Management Manual (SIMM) Section 5300.

State Entities must adhere to OIS-issued information security and privacy policies and all relevant laws, regulations, rules, and standards governing their State Entity. Compliance may be reflected in audit findings and maturity scores. Non-compliance will be addressed according to the Information Security Policy Compliance and Enforcement Standard (SIMM 5330-H).

As described in GC Section 11549.3.(f) (2), a state agency as defined in GC Section 11000 that is not under the direct authority of the Governor may adopt and implement this policy voluntarily. Such a state agency may discontinue use of this policy at any time.

Definitions

OIS uses SAM 5300 definitions, as well as approved authoritative sources for terms not defined in SAM 5300. For the purposes of SIMM 5340-A, the following definitions apply:

State Entity – As defined in SAM 5300.4.

Incident - An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. (synonymous with Security Incident in SAM 5300.4)

Incident Response Plan (IRP) - The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of malicious cyberattacks against an organization's information assets.

Personal Information (PI) – As defined in Civil Code 1798.3 and 1798.29.

Incident Response Plan

Plan Elements

Per SAM 5340, Information Security Incident Management, State Entities must develop, disseminate, and maintain a written Incident Response Plan (IRP) which must be reviewed and updated annually. In the event of any changes to relevant processes or personnel, the plan must be updated promptly and not deferred until the annual review. Additionally, State Entities are required to conduct annual tabletop exercises to ensure all elements of the plan are accurate, current, and realistic. The IRP will provide a structured approach to identifying, reporting, responding to, mitigating, and recovering from security Incidents to minimize damage and reduce downtime to State Entities' systems, data, and operations, especially those designated in their TRP.

In addition to the requirements in SAM 5340, The IRP must include the following within the plan itself or as addenda:

- Clearly defined roles and responsibilities of individuals involved in Incident response, including decision-making authority and communication channels, and escalation procedures with communication thresholds as defined by your organization. Additionally, the IRP must list appropriate roles which must have California Compliance and Security Incident Reporting System (Cal-CSIRS) accounts and permissions for Incident reporting.
- Detection, monitoring, investigating alerts, and incident reporting roles are defined, and workflows, processes/procedures, and responsibilities for each are documented.
- Dedicated Incident response playbooks that outline detailed containment and eradication steps to isolate and contain an Incident, mitigate damage, and remove the threat from affected systems.
- Guidelines for preserving evidence and chain of custody and analyzing incidents to identify root causes and prevent future occurrences.
- A communication plan that specifically defines communication requirements and workflows with regulatory bodies, the public, and internal and external stakeholders throughout the different phases of an Incident.
- Steps for restoring non-essential systems and data, and guidance for initiating the State Entity's Technology Recovery Plan (TRP) and Continuity Plan (CP) when an Incident escalates to a level requiring formal recovery activation.
- A process for assessing Incident response effectiveness and identifying areas for improvement. The process should include documenting findings and lessons learned to apply those findings to applicable State Entity program management documents and playbooks.

All documentation developed to support the IRP should be customized for the specific State Entity. If a State Entity has an established Supported Services relationship with another State Entity as defined in SIMM 5330-A Designation Letter, the hosted or client State Entity may inherit the host/steward's IRP.

Plan Procedures

In addition to the specified IRP elements, every State Entity must establish and maintain the two following categories of procedures in the IRP:

- Procedures for ensuring Incidents involving loss, damage, theft, misuse of information assets, or improper dissemination of information are promptly investigated.
- Procedures to ensure that any breach of security involving PI, regardless of its medium (e.g., paper, electronic, verbal), is reported and handled as quickly and efficiently as possible.

The State Entity's procedures must be documented in the IRP and include the following minimum required elements:

1.	**State Entity Incident Response Team**	A State Entity's response team should include, but is not limited to, the following: • Incident Response Team Leader / Escalation Manager • Program Manager of the program or office experiencing the Incident or breach • Information Security Officer (ISO) • Chief Information Officer (CIO) • Agency Information Security Officer (AISO) (if applicable) • Chief Privacy Officer/Coordinator (CPO/CPC) or Senior Official for Privacy

		• Public Information or Communications Officer • In-house Legal Counsel • Others applicable to the Incident or as directed by the OIS The Escalation Manager, usually the ISO or CPO/CPC, ensures that appropriate representatives from across the organization are involved in completing the process. Additional personnel may be involved in some Incidents.
2.	**Protocol for Internal and External Communications**	The IRP must ensure that a communication flow is defined between management and employees, external vendors, and other organizations such as Cal-CSIRS, the California Governor's Office of Emergency Services, law enforcement agencies, and other State Entities. This ensures that executive management and the Incident response team can respond promptly. The plan must include instructions for communicating up the chain of command to the State CIO's Directorate Office, Cabinet Secretary, and the Governor's Office when necessary. Additionally, it must establish a central point of contact for media and customer inquiries.

3.	**Protocol for the Incident Lifecycle**	The IRP must include a detailed description of all phases of an Incident's lifecycle, including Incident Response (CSF 2.0 Functions Detect, Respond, Recover), Lessons Learned (Identify – Improvement), and Preparation (Govern, Identify, Protect). These phases were previously Preparation, Detection and Analysis, Containment, Eradication & Recovery, and Post-Incident Activity, which are mapped to CSF 2.0 Functions in NIST SP 800-61 Rev. 3.
4.	**Protocol for Preservation of Evidence**	The IRP must include guidance on preserving evidence, such as system images, artifacts and Indicators Of Compromise (IOCs), during and after an Incident, for transfer to appropriate authorities for criminal investigation and to assess the Incident's scope, attribution, and remediation. The IRP must include guidelines on monitoring and maintaining the chain of custody of potentially compromised systems or data and it must require State Entities to gain approval from the California Cybersecurity Integration Center (Cal-CSIC) or (if requested) the California Highway Patrol (CHP) Computer Crimes Investigation Unit (CCIU) before system reimaging.

Decision-Making Criteria and Protocol for Notifying Individuals

A State Entity's IRP must include documentation of the methods and criteria that align with Civil Code Section 1798.29 and SIMM 5340-C for determining when and how a notification to external parties such as data breach victims will be made.

The IRP must consistently comply with applicable laws and state policies. At a minimum, a State Entity's IRP will address the following elements:

- Whether the notification is required by law.
- Whether the notification is required by state policy.
- Timeliness of notification.
- Source of notice.
- Content of notice.
- Approval of notice before release.
- Method(s) of notification.
- Preparation for follow-on inquiries.
- Other actions the State Entity can take to mitigate harm to individuals.
- Other situations when notification should be considered.

SIMM 5340-C, Requirements to Respond to Incidents Involving a Breach of Personal Information, outlines a more detailed description of these elements for incidents involving PI. See section “Special Handling Instructions for Incidents Involving Personal Information” below.

State Entities requiring assistance developing their IRP may contact the California Department of Technology’s (CDT) Advisory Services Program. The program can consult with the State Entity and provide templates to ensure compliance with this standard.

Incident Reporting

What Makes an Event a Reportable Incident

An event, such as system failure, outage, error, or unusual or unexpected behavior may or may not be incident. As defined above, if security policy or the confidentiality, integrity, or availability of a system or data is violated, it is likely an Incident. See more specific examples in the Reporting Criteria section below. Once any State Entity staff determine that an event or occurrence is an Incident, prompt and appropriate reporting is necessary.

Reporting Incidents is essential for quickly identifying and mitigating risks to prevent further damage to systems, data, and operations. It promotes accountability, compliance, and ongoing improvement in a State Entity's security posture.

State Entities informed of Incidents through notifications from law enforcement or other trusted third parties, including any related and open criminal or federal cases, must also report such Incidents in Cal-CSIRS.

Any Incident involving PI may require the agency to notify the affected individuals and additional applicable reporting agencies, as further detailed in SIMM 5340-C.

State Entities are to consult the California Health and Human Services Agency (CalHHS) about whether they are subject to the Health Insurance Portability Accountability Act (HIPAA) requirements and any additional reporting responsibilities associated with a breach of personal health information. Additional information is available on the CalHHS website at https://www.chhs.ca.gov/

Additionally, covered entities will be required to report covered cyber incidents and ransomware payments that impact critical infrastructure to the U.S. Cybersecurity and Infrastructure Agency (CISA), as required in the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), and upcoming regulations. For more information see https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia. In the meantime, for any type of Incident, CISA encourages reporting to https://www.cisa.gov/report.

When To Report – Incident Reporting Timeline

Upon discovery of an Incident, the State Entity must immediately report it through Cal-CSIRS. Timely reporting is essential to limit potential propagation to other State departments and allied agencies and to help minimize overall risk.

A reported Incident should provide sufficient details (mandatory fields) so an Incident report can be closed in a timely manner. Updates, including any requested clarifications, must be provided every 48 hours unless otherwise directed by OIS. If the resolution extends beyond 10 business days, the updated closure date must be recorded in Cal-CSIRS.

Before closure of an Incident, a State Entity must complete mandatory fields required for the Incident, including financial loss and corrective actions taken to identify and mitigate the root cause of the Incident to minimize recurrence. If corrective actions cannot be completed immediately, they must be documented in the State Entity's Risk Register and Plan of Action and Milestones (RRPOAM). State Entities are required to maintain a procedure to track all security events, Incident reports, and non-reportable incidents (e.g. false positives).

What To Report (Reporting Criteria)

Incidents that must be reported through Cal-CSIRS to OIS, Cal-CSIC, and the CHP CCIU include, but are not limited to, the following:

- Theft, loss, damage, unauthorized destruction, unauthorized modification, or unintentional or inappropriate release of any data classified as confidential, sensitive, or personal.
    - Possible acquisition of notice-triggering PI, as defined in Civil Code 1798.29, by unauthorized persons.
    - Deliberate or accidental distribution or release of personal information by a State Entity or its personnel in a manner not in accordance with law or policy.

    - Entering confidential data into publicly accessible AI tools, platforms not solely owned and operated by the organization, which may cause or lead to unauthorized disclosure.
    - Intentional non-compliance with State Entity or state information security or privacy policy by the responsible custodian of information.
- **Criminal Activity** - Use of a state information asset in the commission of a crime as described in the Comprehensive Computer Data Access and Fraud Act. See Penal Code Section 502.
- **Unauthorized Access** - Actions of State Entity personnel and/or unauthorized individuals that involve tampering, interference, damage, or unauthorized access to state computer data and computer systems.
- **Cyberattacks** - This includes, but is not limited to, successful virus attacks or exploited vulnerabilities, website defacements, and denial of service attacks.
- **Equipment** - This includes theft, damage, destruction, or loss of state-owned Information Technology (IT) equipment, including laptops, tablets, integrated phones, smart phones, or any electronic devices containing or storing confidential, sensitive, or personal data.
- **Inappropriate Use -** This includes circumventing information security controls or misuse of a state information asset by State Entity personnel and/or any unauthorized individuals for personal gain and/or engaging in unauthorized peer-to-peer activity, obscene, harassing, fraudulent, illegal**,** or other inappropriate activity.
- **Outages and Disruptions** - Any outage or disruption to a State Entity's mission-critical systems or public-facing web applications lasting more than two hours or in which the Incident triggers the State Entity's emergency response or technology recovery.
- Any other Incidents that violate State Entity information security or privacy policy.

How To Report Incidents

Any actual (true positive) or suspected Incident that meets reporting criteria in any type of media (e.g., electronic, paper) must be reported immediately through Cal-CSIRS.

Information about how to use and access Cal-CSIRS can be found on the OIS Security Policy Website. Representatives from OIS, Cal-CSIC, and/or CHP CCIU will contact the State Entity as soon as possible after receiving the Cal-CSIRS notification.

IMPORTANT: A REPORT MADE TO CHP, OTHER LAW ENFORCEMENT AGENCIES, OR OIS OUTSIDE OF THE CAL-CSIRS NOTIFICATION PROCESS BY EMAIL OR OTHER MEANS IS NOT AN ACCEPTABLE SUBSTITUTE FOR THE REQUIRED REPORT THROUGH CAL-CSIRS.

If the Cal-CSIRS system is offline or you are unable to access Cal-CSIRS, contact OIS directly during regular business hours by phone at (916) 245-2583 or by e-mail at security@state.ca.gov for assistance and Cal-CSIC via calcsic_watch@caloes.ca.gov at (833) REPORT-1 or (916) 636-2997.

If the Cal-CSIRS system is offline outside of regular business hours and you need immediate law enforcement assistance, contact CHP's Emergency Notification and Tactical Alert Center (ENTAC) at (916) 843-4199. ENTAC is operational 24/7, and the officers at ENTAC will forward that information to CCIU for immediate assistance. If the notification is made outside of regular business hours through ENTAC, the State Entity is responsible for notifying OIS of the Incident the next business day.

Reporting Instructions Using Cal-CSIRS

When reporting an Incident, Cal-CSIRS requires specific information, and all mandatory fields must be completed.

Once all mandatory fields are completed and the Incident is submitted, an automated workflow notifies OIS, Cal-CSIC, and CHP CCIU. The Incident reporter will receive a system-generated email confirmation acknowledging receipt by OIS, Cal-CSIC, and CHP CCIU. If applicable, OIS and/or Cal-CSIC will schedule a briefing call to discuss action items and provide guidance or assistance as needed.

All Cal-CSIRS information is Confidential and Exempt and is not subject to the Public Records Act (PRA) per GC Section 7929.210(a). **IMPORTANT: A Cal-CSIRS Incident must be opened immediately upon discovering a breach.**

In addition to the system-generated fields, the ISO or delegated Cal-CSIRS user should attempt to create an Incident record containing as much of the following information, including mandatory fields, as possible.

Completeness of this information should not delay reporting the Incident in Cal-CSIRS as timely communication is the most important factor when reporting an Incident. Prioritize first creating an incident report promptly with the mandatory fields completed and as much readily available information from the list below as possible. Then continue to update the report as additional information is found.

- Name and address of the reporting State Entity.
- Name, address, e-mail address, and phone number(s) of the reporting person.
- Name, address, e-mail address, and phone number(s) of the ISO.
- Name, address, e-mail address, and phone number(s) of the alternate contact.
- ISO, system administrator, etc.
- Detailed description of the Incident.
- Date and time the Incident occurred.
- Date and time the Incident was discovered.
- Make / model of the affected device(s).
- IP address of the affected device(s).
- Assigned name of the affected device(s).
- Operating system of the affected device(s).
- Location of the affected device(s).
- Actions taken before reporting on Cal-CSIRS.

Additional guidance for reporting the Incident can be found on the CHP's Computer Crime Reporting for State Agencies webpage.

The CHP CCIU, Cal-CSIC, and/or OIS may contact the State Entity for additional information for further investigation.

Special Handling Instructions for Incidents Involving Personal Information

It is required to indicate if the Incident involves a breach of notice-triggering PI. If any type of PI as defined in Civil Code Section 1798.29 is involved, State Entities must reference SIMM 5340-C for guidelines and templates on breach notifications to impacted parties to ensure compliance with California Civil Code 1798.29.

Notice to Affected Individuals

Notification must be given to affected individuals when there is a breach of unencrypted data elements that trigger notification requirements, regardless of whether the data is in electronic or paper format and according to the established criteria.

OIS Prior Review and Approval of Breach Notice:

The draft of the breach notification must be uploaded into the reported Incident created through Cal-CSIRS for OIS to review and approve. As outlined in SIMM 5340-C, OIS reviews and must approve the breach notice before its release to any individual.

Activation of Technology Recovery / Continuity Plan(s)

In the event of destruction, degradation, corruption, or loss (due to physical or virtual unavailability) of systems identified as critical, State Entities should refer to the procedures maintained within their Technology Recovery Plan (TRP), which describe how these systems will fail over to known good environments and/or recover within established minimum recovery times. State Entities must also demonstrate the effectiveness of these plans through adequate training and preparation, such as annual recovery exercises. See SAM 5325 and SIMM 5325-A/B.

Unavailability may also occur due to legal requirements such as criminal investigations. If a criminal investigation arises from an Incident, State Entities must provide replacement or temporary loaner devices for affected customers. Production-level systems should have backup systems to ensure business continuity until the affected system is confirmed, by the Cal-CSIC and/or CCIU, that no further evidence or artifacts are needed for investigative and forensic purposes before system restoration.

Upon containment and eradication of an Incident, the State Entity must activate TRP and CP activities as appropriate to the Incident to ensure all systems, data, and business processes are restored according to recovery time objectives (RTOs), recovery point objectives (RPOs), and recovery prioritization criteria. State Entities are then to monitor the previously affected systems to ensure system activity is back to normal operations.

State Entities that experience ransomware attacks are prohibited from paying any form of ransom for recovery keys to their data until they have formally consulted with the Cal-CSIC and the Federal Bureau of Investigation (FBI).

Incident Closure

Once all information assets have been fully recovered, the Incident can be approved for closure and returned to a protection-level state with the approval of OIS. The affected State Entity must submit a report of their investigation through Cal-CSIRS, with a post-Incident timeline detailing the Incident's scope, impact, root cause, and corrective actions. Additionally, all data and financial fields in the Cal-CSIRS Incident must be completed before requesting closure.

State Entities must ensure that no outstanding Incidents are open and left unaddressed in Cal-CSIRS. Other than OIS's prior approval of an extension on major Incidents,

State Entities are to further conduct annual reviews on previous Incidents, to further mature their information security program by detecting and remediating potential systemic issues that would mitigate similar Incidents in the future.

NIST CSF Functions

Function	Category
Govern (GV)	• GV.OC: Organizational Context • GV.OV: Oversight • GV. PO: Policy

	• GV.RR: Roles, Responsibilities, and Authorities • GV.RM: Risk Management Strategy • GV.SC: Cybersecurity Supply Chain Risk Management
Identify (ID)	• ID.AM: Asset Management • ID.IM: Improvement • ID.RA: Risk Assessment
Protect (PR)	• PR.AA: Identity Management, Authentication, and Access Control • PR.AT: Awareness and Training • PR.DS: Data Security • PR.PS: Platform Security • PR.IR: Technology Infrastructure Resilience
Detect (DE)	• DE.AE: Adverse Event Analysis • DE.CM: Continuous Monitoring
Respond (RE)	• RS.MA: Incident Management • RS.AN: Incident Analysis • RS.CO: Incident Response Reporting and Response • RS.MI: Incident Mitigation
Recover (RC)	• RC.RP Incident Recovery Plan Execution • RC.CO: Incident Recovery Communication

References

- Office of Information Security: https://cdt.ca.gov/security/

- Information about how to use and access Cal-CSIRS can be found on the OIS Security Policy Website: https://cdt.ca.gov/security/policy/
- California Highway Patrol Reporting Requirements (Government Code 14613.7): https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=GOV&sectionNum=14613.7
- California Information Practices Act (Civil Code Sections 1798.29): https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.29.&lawCode=CIV
- Computer Crime Reporting for State Agencies: https://www.chp.ca.gov/Notify-CHP/Computer-Crime-Reporting-For-State-Agencies
- NIST SP 800-61 Rev. 3 Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile: https://csrc.nist.gov/pubs/sp/800/61/r3/final
- Cyber Incident Reporting Critical Infrastructure Act (CIRCIA): https://www.congress.gov/bill/117th-congress/house-bill/2471/text\

  https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia
- National Security Memorandum on Critical Infrastructure Security and Resilience (NSM-22): https://www.cisa.gov/national-security-memorandum-critical-infrastructure-security-and-resilience
- CISA National Cyber Incident Scoring System (NCISS): https://www.cisa.gov/news-events/news/cisa-national-cyber-incident-scoring-system-nciss
- CISA Tabletop Exercise Packages: https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages
- SAM 5300 Definitions: https://cdt.ca.gov/security/technical-definitions/
- SIMM Section 5300: https://cdt.ca.gov/policy/simm/

- Unauthorized Computer Access (Penal Code § 502): https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=502.&lawCode=PEN