
State of California
California Information Security Office
Incident Reporting and Response
Instructions

SIMM 5340-A

May 2016

REVISION HISTORY

REVISION	DATE OF RELEASE	OWNER	SUMMARY OF CHANGES
Initial Release	August 2012	California Office of Information Security	
Minor Update	September 2013	California Information Security Office (CISO)	SIMM number change, transferred procedural content from State Administrative Manual (SAM), Chapter 5300
Update	May 2016	CISO	Update incident reporting instructions for the SIMM 5340-B: eliminating incident reporting through ENTAC; directing all incident reports to be made through the Cal-CSIRS system

TABLE OF CONTENTS

INTRODUCTION.....	1
REPORTING CRITERIA.....	1
INCIDENT NOTIFICATION.....	2
INCIDENT HANDLING AND RESPONSE.....	3
SPECIAL HANDLING INSTRUCTIONS FOR INCIDENTS INVOLVING PERSONAL INFORMATION.....	4
INCIDENT REPORTING.....	5

INTRODUCTION

State entity management must promptly investigate incidents involving loss, damage, misuse of information assets, or improper dissemination of information. All entities are required to report information security incidents in accordance with the security notification and reporting requirements in these instructions.

Proper incident management includes the formulation and adoption of a written incident management plan that provides for the timely assembly of appropriate staff that are capable of developing a response to, appropriate reporting about, and successful recovery from a variety of incidents.

In addition, incident management includes the application of lessons learned from incidents, together with the development and implementation of appropriate corrective actions directed to preventing or mitigating the risk of similar occurrences in the future.

Upon discovery of any incident that meets the notification and reporting criteria defined herein, all state entities must immediately report the incident following these Information instructions.

REPORTING CRITERIA

An incident is 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.

Incidents which must be reported to the California Information Security Office (CISO) and the California Highway Patrol (CHP) Computer Crimes Investigation Unit (CCIU) immediately following discovery include, but are not limited to, the following:

1. **State Data** (includes electronic, paper, or any other medium)-
 - a. Theft, loss, damage, unauthorized destruction, unauthorized modification, or unintentional or inappropriate release of any data classified as confidential, sensitive or personal.
 - b. Possible acquisition of notice-triggering personal information by unauthorized persons, as defined in [Civil Code 1798.29](#).
 - c. 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.
 - d. Intentional non-compliance by the custodian of information with his/her responsibilities.
2. **Criminal Activity** - Use of a state information asset in commission of a crime as described in the Comprehensive Computer Data Access and Fraud Act. See [Penal Code Section 502](#).
 - a. **Unauthorized Access** - This includes actions of state entity personnel and/or unauthorized individuals that involve tampering, interference, damage, or unauthorized access to state computer data and computer systems.

- b. **Attacks** - This includes, but is not limited to, successful virus attacks or exploited vulnerability, web site defacements, and denial of service attacks.
3. **Equipment** – This includes theft, damage, destruction, or loss of state-owned Information Technology (IT) equipment, including laptops, tablets, integrated phones, personal digital assistants (PDA), or any electronic devices containing or storing confidential, sensitive, or personal data.
4. **Inappropriate Use** – This includes the circumventing of information security controls or misuse of a state information asset by state entity personnel and/or any unauthorized individuals for personal gain, or to engage in unauthorized peer-to-peer activity, obscene, harassing, fraudulent, illegal or other inappropriate activity
5. **Outages and Disruptions** – This includes any outage or disruption to a state entity’s mission critical systems or public-facing web applications lasting more than 2-hours, or in which the incident triggers the state entity’s emergency response or technology recovery.
6. **Any other incidents that violate state entity information security or privacy policy.**

INCIDENT NOTIFICATION

State policy requires state entities to make notification to CISO and CHP immediately following discovery of an incident. Each state entity's Chief Information Officer (CIO), Information Security Officer (ISO), or the assigned incident reporting personnel, collectively hereinafter referred to as authorized California Compliance and Security Incident Reporting System (Cal-CSIRS) user, is responsible for notifying the proper authorities following these steps:

Responsibility of the state entity ISO or authorized Cal-CSIR user:

Immediately report the incident through the Cal-CSIRS. Cal-CSIRS will require specific information about the incident and will notify the CISO and the CHP Computer Crimes Investigation Unit (CCIU). A system generated e-mail confirmation will be sent to the authorized Cal-CSIRS users acknowledging the CISO and CCIU have received the Cal-CSIRS notification.

IMPORTANT: The ISO or authorized Cal-CSIRS user should attempt to gather the following information before creating an incident report in Cal-CSIRS; however, if the information is not available, notification should not be delayed:

- 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 (e.g., alternate ISO, system administrator, etc.)
- Description of the incident
- Date and time the incident occurred
- Date and time the incident was discovered
- Make / model of the affected computer(s)

- IP address of the affected computer(s)
- Assigned name of the affected computer(s)
- Operating system of the affected computer(s)
- Location of the affected computer(s)
- Actions taken prior to reporting on Cal-CSIRS

Additional guidance for reporting the incident can be found on the [“Computer Crime Reporting for State Agencies”](#) page located on the CHP Web site.

During this notification process, it is important to indicate if the incident involves personally identifiable information, such as notice-triggering personal information, protected health information, or electronic health information.

The CHP CCIU and/or the CISO may contact the state entity for additional information or further investigation.

INCIDENT HANDLING AND RESPONSE

Every state shall establish and maintain in its incident management plan and procedures for: 1) ensuring incidents involving loss, damage, misuse of information assets, or improper dissemination of information are promptly investigated; and, 2) ensuring that any breach of security involving personal information, regardless of its medium (e.g., paper, electronic, verbal) are reported and handled in the most expeditious and efficient manner.

The state entity's procedures must be documented and address, at a minimum, the following:

1. State entity Incident Response Team.

A state entity's procedures shall identify the positions responsible for responding to incidents and a breach of personal information. A state entity's response team must include, at a minimum, the following:

- an escalation manager,
- the Program Manager of the program or office experiencing the incident or breach,
- the Information Security Officer (ISO),
- the Chief Privacy Officer/Coordinator (CPO) or Senior Official for Privacy,
- the Public Information or Communications Officer,
- Legal Counsel, and
- others as directed by the CISO.

The escalation manager, often the ISO or CPO, is responsible for ensuring appropriate representatives from across the organization are involved and driving the process to completion. Some incidents will require the involvement of others not mentioned above. For example, if the source of the compromised information was a computer system or database, the Chief Information Officer should also be involved in the response activity. If the incident involves unauthorized access, misuse, or other inappropriate behavior by a state employee, or the security breach involves state employee's personal information, the state entity's Personnel Officer or

Human Resource Manager should be involved. Furthermore, if the incident involves multiple state entities, the response team from each state entity may be involved.

2. Protocol for Internal and External Communications.

A state entity's procedures shall outline the method, manner, and progression of internal reporting, as to ensure that executive management is informed about incidents and breaches involving personal information, and the state entity's Incident Response Team is assembled and the incident is addressed in the most expeditious and efficient manner. The state entity's procedures shall include instructions for communicating up its chain of command to Cabinet-Secretary and the Governor's Office when necessary and establishing the central point of contact for media inquiries.

3. Protocol for Preservation of Evidence.

The state entity's plan and procedures shall provide instruction to incident response teams and other personnel which may be involved in the response investigation of an incident for working with and through law enforcement to preserve evidence, and maintain both chain of custody and chain of evidence.

Protocol for Security Incident Reporting:

Any actual or suspected incident meeting the criteria described earlier or breach of personal information (notice-triggering and non-notice-triggering data elements) in any type of media (e.g., electronic, paper) is to be reported immediately to CISO and CHP CCIU through Cal-CSIRS. Representatives from the CISO and/or CHP CCIU will contact the state entity as soon as possible following their receipt of the Cal-CSIRS notification.

IMPORTANT: A report made to CHP, other law enforcement agencies, or the CISO outside of the Cal-CSIRS notification process by email or other means is NOT an acceptable substitute for the required report through Cal-CSIRS.

In the case that the Cal-CSIRS system is offline during normal business hours, contact CISO directly by phone at (916) 445-5239 or by e-mail at security@state.ca.gov for assistance. If the Cal-CSIRS system is offline outside of normal business hours and you require immediate law enforcement assistance, contact CHP's Emergency Notification and Tactical Alert Center (ENTAC) at (916) 843-4199. This telephone number is staffed 24-hours a day, seven days a week. The officers at ENTAC will forward that information to CCIU for immediate assistance. In the situation that notification is made outside of normal business hours through CHP, it is the state entity's responsibility to notify CISO of the incident the next business day.

SPECIAL HANDLING INSTRUCTIONS FOR INCIDENTS INVOLVING PERSONAL INFORMATION

Decision Making Criteria and Protocol for Notifying Individuals:

A state entity's procedures shall include documentation of the methods and manner for determining when and how a notification is to be made. The procedures shall be consistent with and comply with applicable laws and state policies. At a minimum, a state entity's procedures will address the following elements:

1. Whether the notification is required by law.
2. Whether the notification is required by state policy.
3. Timeliness of notification.
4. Source of notice.
5. Content of notice.
6. Approval of notice prior to release.
7. Method(s) of notification.
8. Preparation for follow-on inquiries.
9. Other actions that state entities can take to mitigate harm to individuals.
10. Other situations when notification should be considered.

A more detailed description of these elements is set forth in the Requirements to Respond to Incidents Involving a Breach of Personal Information ([SIMM 5340-C](#)).

Notice to Affected Individuals:

Notice to individuals when a breach of unencrypted notice-triggering data elements occurs, regardless of the media involved (electronic or paper), and in accordance with criteria set forth above.

CISO Prior Review and Approval of Breach Notice:

The draft of the breach notification must be uploaded into the incident report created through Cal-CSIRS for the CISO Program Manager to review and approve. The CISO provides review and must approve the breach notice prior to its release to any individual as set forth in Requirements to Respond to Incidents Involving a Breach of Personal Information ([SIMM 5340-C](#)).

INCIDENT REPORTING

The Cal-CSIRS ([SIMM 5340-B](#)), is available via the CISO's website at <http://www.cio.ca.gov/OIS/Government/policy.asp>. The report must be created and submitted through Cal-CSIRS upon the state entity's becoming aware of an incident.

A state entity report must outline the details of the incident and corrective actions taken, or to be taken, to address the root cause of the incident. The report must be completed through Cal-CSIRS within 10 business days following creation of the incident. If corrective actions cannot be completed immediately, follow the instructions outlined in [SIMM 5305-B](#) to submit a Plan of Actions and Milestones ([SIMM 5305-C](#)) that identifies all corrective actions along with timelines indicating when these corrective actions will be completed. If the state entity currently has a POAM on file, you will need to update the existing POAM and resubmit.

Further, any incident involving personal identifying information may require the state entity to notify the effected individuals and additional reporting may be necessary for state entities that must adhere to Health Insurance portability and Accountability Act (HIPAA) requirements. State entities are to consult the California Office of Health Information Integrity (CalOHII) about whether or not they are subject to the HIPAA requirements and any additional reporting responsibilities associated with a breach of personal medical or health information. Additional information is available on the CalOHII website at <http://www.ohi.ca.gov/calohi/state-departments.htm>.

The Office may require that the state entity provide additional information in conjunction with its assessment of the incident.

Questions regarding the notification or reporting process may be directed to security@state.ca.gov or by calling (916) 445-5239.