



## Important Contact Information



## Incident Notification and Reporting

The **California Information Security Office (CISO)** provides policy direction and oversight of state government's protection of information assets.

(916) 445-5239  
[www.infosecurity.ca.gov](http://www.infosecurity.ca.gov)

The **California Highway Patrol (CHP)** provides intake and notification support for initial calls from state entities as they relate to information security incidents. CHP has primary responsibility for investigations involving computer crimes and any other crimes against state assets.

(916) 843-4199  
[www.chp.ca.gov](http://www.chp.ca.gov)

The **California Office of Health Information Integrity (CalOHII)** directs and tracks additional incident reporting requirements for Health Insurance and Portability Accountability Act (HIPAA) impacted entities.

(916) 651-6907  
[www.calohi.ca.gov](http://www.calohi.ca.gov)

The **California Office of the Attorney General (OAG)** enforces state and federal privacy laws, and tracks data breaches involving notification to 500 or more individuals.

[www.privacy.ca.gov](http://www.privacy.ca.gov)

The State Administrative Manual (SAM) Section 5340 requires state entities to notify and report suspected or actual information security incidents immediately upon discovery.

Typically, it is the responsibility of each state entity's Information Security Officer, or their designated backup, to notify the proper authorities of an incident by following these steps:

1. State entity notifies the CHP ENTAC immediately upon discovery of the incident. The 24-hour phone line is **(916) 843-4199**.
2. The CISO and, in some cases, CHP's Computer Crimes Investigation Unit (CCIU) will contact the state entity for additional details regarding the incident and to provide assistance as needed.
3. State entity takes immediate steps to resolve the issue and, if necessary, makes notification to affected individuals in accordance with documented procedures (SIMM 5340-A and SIMM 5340-C).
4. The state entity completes and submits the follow-up written security incident report (SIMM 5340-B) to the CISO within 10 business days from the date of the notification to CHPENTAC.
5. State entity implements corrective action steps identified in the report to rectify or mitigate the incident so it will not recur.

**California Information Security Office**  
Phone: (916) 445-5239  
Email: [security@state.ca.gov](mailto:security@state.ca.gov)  
Web: [www.infosecurity.ca.gov](http://www.infosecurity.ca.gov)



LEADING THE WAY TO SECURE THE  
STATE'S INFORMATION ASSETS

# INFORMATION SECURITY INCIDENT REPORTING ROADMAP FOR STATE GOVERNMENT

Prepared by the  
California Information Security Office  
December 2014

# FAQS FOR INFORMATION SECURITY INCIDENTS



**REPORT INCIDENTS IMMEDIATELY!**

## What is an Information Security Incident?

An event that is reasonably believed to have compromised the confidentiality, integrity, or availability of an information asset or an information system (automated or paper) that processes, stores, or transmits information; or, an event that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

## What are some examples?

A complete list of reporting requirements and criteria is found in Incident Reporting and Response Instructions (SIMM 5340-A) procedures. However, the following are examples of a reportable incident:

- Theft, loss, damage, unauthorized destruction or modification of information, or unintentional or inappropriate release of confidential, personal, or sensitive (C/P/S) information (paper or electronic).
- Inappropriate use of an information asset, unauthorized access by a contractor or employee, or access that exceeds authorized limits.
- Loss or theft of any IT equipment including desktops, laptops, PDAs, or any electronic media capable of containing or storing information.
- Criminal activity such as piracy, copyright infringement, and successful system or application hacks, exploited vulnerabilities, website defacements, virus attacks, and denial of service attacks. Service levels are usually, but not always, impacted by these types of events.
- Violations of state security policy such as downloading, storing, or viewing inappropriate or illegal material on state systems.

## Who should call the California Highway Patrol (CHP) Emergency Notification and Tactical Alert Center (ENTAC) to report the incident?

Typically, the state entity's Information Security Officer (ISO), or his or her backup, calls CHP ENTAC to report the incident.

## What if I am not sure it is an incident or if CHP ENTAC does not take the report?

Call the California Information Security Office (CISO) as soon as possible at (916) 445-5239.

## What information should the entity's ISO or reporting individual making the notification be prepared to provide when calling CHP ENTAC?

Important things to be prepared to provide include:

- The reporting entity's name.
- The reporting person's contact information.
- The ISO and designated backup contact information.
- A description of incident.
- The date and time the incident *occurred*.
- The date and time the incident was *discovered*.
- Whether paper or electronic records were impacted.
- Whether the records contained C/P/S information.
- If known, how many records and individuals were impacted?
- If personal information was involved, whether the state entity has or will be notifying the affected individuals.
- When applicable, the make/model and IP address of the affected system, computer, electronic device, or media.
- Whether the electronic device or media, or the C/P/S information on the device or media, was encrypted and/or password protected.



## What are the state entity's responsibilities if the incident involves the theft or loss of personal information?

Besides reporting the incident to the CHP and CISO, the state entity may be required by law to notify the affected individuals that their personal information has been lost or stolen. The Information Practices Act (Civil Code 1798 et seq.) defines a notice triggering event. Oftentimes, however, there is good reason to notify the affected individuals even if it is not required by law. Notification is made in accordance with Requirements to Respond to Incidents Involving a Breach of Personal Information (SIMM 5340-C) procedures.

## What resources are available to a state entity for assistance in handling an incident involving personal information?

The CISO and CHP provide direction and assistance in handling any type of information security incident. See the reverse side of this brochure for contact information.

## Who else should the incident be reported to?

Depending upon the internal plan, its severity or if it has the capacity of becoming a high profile event, the state entity may need to notify its cabinet-level management and its communications/public information officer. HIPAA-impacted entities must notify California Office of Health Information Integrity (CalOHII), and the California Office of the Attorney General (OAG) must be notified when the incident results in breach notification delivery to 500 or more individuals.

## Now that the incident has been reported to CHP ENTAC, what are the state entity's responsibilities?

First and foremost, the state entity must work cooperatively with CHP and CISO, and take steps to resolve the issue. Then a Security Incident Report (SIMM 5340-B) must be completed, signed by the head of the state entity, and submitted to the CISO within 10 business days of incident reporting. The corrective action plan identified in the report must be completed to mitigate risk of recurrence.

## Where do I find the Security Incident Report (SIMM 5340-B)?

It is located on the CISO's website at [www.infosecurity.ca.gov](http://www.infosecurity.ca.gov).

## What is an Incident Response Plan (IRP)?

This is an internal state entity plan, in compliance with statewide incident management requirements, that identifies actions its employees must follow when an incident occurs. It contains important contact information and procedures to be followed for properly handling various types of incidents. State entities must develop, implement, and ensure all employees are aware of this plan BEFORE an incident occurs.

## What resources are available to aid a state entity in developing an IRP?

Information regarding the development of an Incident Response Plan is available on the CISO's website at [www.infosecurity.ca.gov](http://www.infosecurity.ca.gov) under Incident Management "Other Resources" or under Quick Links in "Samples and Templates".

## My question was not addressed in this FAQ. Is more information available elsewhere?

Yes, on the CISO's website at [www.infosecurity.ca.gov](http://www.infosecurity.ca.gov).

