INFORMATION SECURITY INCIDENT REPORTING 0938

(No.32 May 2015)

The California Department of Forestry and Fire Protection (CAL FIRE) Information Security Office (ISO) is required to promptly investigate incidents involving loss, damage, misuse of information assets, or improper dissemination of information. Furthermore, the CAL FIRE ISO is required to report information security incidents in accordance with State of California security notification and reporting requirements. If the security incident is related to information assets and/or systems, the CAL FIRE ISO works in collaboration with CAL FIRE Information Technology Services (ITS) to ensure timely response to mitigate the threat effectively and efficiently.

REFERENCE(S) 0938.1

(No.32 May 2015)

California Information Security Office (CISO) SIMM 5340-A, 5340-B, 5340-C
Civil Code (CC) 1798.29
Penal Code Section 502
State Administrative Manual 5340 et seq.
Management Memo 08-11
National Institute of Standards and Technology SP 800-53: Incident Response

GENERAL PROVISIONS 0938.2

(No.32 May 2015)

An information security 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. Examples of information security incidents that are reportable include:

- State Data (includes electronic, paper, or any other medium).
    - 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 personal information by unauthorized persons, as defined in CC 1798.29.
    - 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.
    - Intentional non-compliance by the 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 (CC 1798.29).
    - 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/or computer systems.
    - Attacks – this includes, but is not limited to, successful virus attacks or exploited vulnerabilities, web site defacements, and denial of service attacks.

- Equipment – Theft, damage, destruction, or loss of State-owned information technology equipment, including laptops, tablets, integrated phones, or any electronic devices containing or storing confidential, sensitive, or personal data.

- Inappropriate Use – 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.

- Outages and Disruptions – Outage or disruption to CAL FIRE's mission critical systems or public-facing web applications lasting more than two hours, or in which the incident triggers CAL FIRE's emergency response or technology recovery.

- Any other incidents that violate State or Departmental policy.

The State of California policy requires the CAL FIRE ISO to make notification to the California Highway Patrol's (CHP's) Emergency Notification and Tactical Alert Center immediately following discovery of an incident. The CAL FIRE ISO also works with the California Natural Resources Agency Information Security Office, CISO, and the CHP Computer Crimes Investigation Unit for reporting requirements.

Depending upon the nature of the incident and the systems affected, the Department may be required to submit additional written reports (e.g., Property Survey Report (STD. 152), Report of Crime or Criminally Caused Property (STD. 99) to other State entities. Further, any incident involving personal identifying information may require notification to affected individuals and additional reporting may be necessary (e.g. Health Insurance Portability and Accountability Act (HIPAA) requirements).

If a reportable incident has occurred, please call the CAL FIRE ISO at (916) 206-5900 immediately to report the incident. If the incident involves an information asset and/or system, please contact the assigned ITS Coordinator and/or ITS Customer Services Manager immediately.

When reporting an information security incident to the CAL FIRE ISO, please provide the following information where applicable:

- Name, address, e-mail address, and telephone number(s) of the reporting person
- Description of the incident (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.)
- Date and time the incident occurred
- Date and time the incident was discovered
- Make/model of the affected computer(s)
- Internet Protocol (IP) address of the affected computer(s)
- Assigned name of the affected computer(s)
- Serial number of the affected computer(s)
- State of California asset tag number of the affected computer(s)
- Operating system of the affected computer(s)
- Location of the affected computer(s)
- Whether or not the data was encrypted
- Actions taken prior to contacting the CAL FIRE ISO

Reporting should NOT be delayed until all of this information is gathered. It is understood that in some circumstances this information may not always be readily available when first reported.

Depending on the size and complexity of the information security incident, an Incident Response Team (IRT) may be activated as part of the Department's Incident Response Plan (see Exhibits) and in accordance with State of California requirements.

The following may comprise an IRT:

- ISO
- Privacy Program Coordinator
- Chief Information Officer (if involving an information asset and/or system)
- Legal Counsel
- Respective Deputy Director and/or Region Chief
- Communications Office

- CISO Representative
- Law Enforcement (if applicable)
- Labor and Human Resource Management (if applicable)
- Equal Employment Opportunity (if applicable)

Some incidents will require the involvement of others not mentioned above, including external resources. Furthermore, if the incident involves multiple State entities, the IRT from each State entity may be involved.

To download a "What is a Reportable Incident" flyer to post, select the link or visit the Exhibits section of the handbook.

For more on information security, please visit the CAL FIRE Intranet under Organization/Director's Office/Information Security Office.

(see next section)

(see HB Table of Contents)

(see Forms or Forms Samples)