CHAPTER 13

CALIFORNIA COMPLIANCE AND SECURITY INCIDENT REPORTING

REVISED NOVEMBER 2016

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 13

COMPLIANCE AND SECURITY INCIDENT REPORTING

1. EMERGENCY NOTIFICATION TACTICAL ALERT CENTER. The Emergency Notification Tactical Alert Center (ENTAC) is designed to be a statewide notification center for emergency incidents, including natural disaster, civil disturbance, terrorism, the protection of the state infrastructure, and other incidents. The ENTAC is available 24 hours a day, seven days a week, to receive notifications.

2. CALIFORNIA COMPLIANCE AND SECURITY INCIDENT REPORTING SYSTEM. The California Compliance and Security Incident Reporting System (Cal-CSIRS) database has been developed to facilitate the rapid reporting and notification of computer-related crimes and information technology (IT) security incidents by state agencies. The Cal-CSIRS database will provide notifications to ENTAC and the Computer Crimes Investigation Unit (CCIU). Information Technology security incidents involving the California Highway Patrol (CHP) shall also be reported to the Department Information Security Officer (ISO).

3. INCIDENTS THAT REQUIRE NOTIFICATION. Notification is required for computer crimes, information asset (paper, microfiche, etc.) security incidents, and IT security incidents. Detailed definitions of IT security incidents and/or computer-related crimes are in the State Administrative Manual, Chapter 5340.4, Incident Reporting, Statewide Information Management Manual (SIMM) 5340-A, Incident Reporting and Response Instructions (refer to Annex A of this chapter), California Penal Code Section 502 (refer to Chapter 12 of this manual, Computer Crimes Investigation Unit, Annex A), and Government Code Section 14613.7 (refer to Annex B of this chapter), with a summary provided below:

   a. State-owned data which is classified as confidential, sensitive, or private information was stolen in conjunction with the theft of a computer or data storage device. Data that is collected during the course of CHP employment activities is considered CHP property regardless of whether it is stored on personally-owned or departmental computers. This data must be safeguarded accordingly.

   b. State-owned or state-managed data, without authorization, was damaged, destroyed, deleted, shared, altered, or copied, or used for non-state business. This includes computer documentation and configuration information, as well as electronic and non-electronic data and reports.

c. Unauthorized parties accessed one or more state computers, computer systems, or computer networks. This includes deliberate and unauthorized uses of state-owned computer services, as well as “hacker attacks.”

d. Someone has accessed and without permission added, altered, damaged, deleted, or destroyed any computer software or computer programs which reside or exist internal or external to a state computer, computer system, or computer network.

e. Disruption of state computer services or denial of computer services occurs in a manner that appears to have been caused by deliberate and unauthorized acts.

f. A contaminant was introduced into any state computer, computer system, or computer network. This includes, but is not limited to viruses, Trojans, worms, and other types of malicious attacks.

g. Internet domain names and/or user account names have been used without permission in connection with the sending of one or more electronic mail messages, and thereby caused damage to a state computer, computer system, or computer network, or misrepresented the state or state employees in electronic communications.

h. Damage or destruction of state information processing facilities has occurred.

i. Physical intrusions into state facilities have occurred that may have resulted in compromise of state data or computer systems.

j. Commanders shall ensure that all computer security-related incidents including lost, stolen, damaged, and destroyed state-owned or state-leased equipment or data are reported immediately and documented appropriately. Additionally, commanders shall ensure incidents involving the loss, theft, or misplacement of unencrypted personal/confidential computer data are reported immediately or as soon as possible pursuant to the requirements of California Civil Code (CIV) 1798.29.

k. Notification and documentation are as follows:

(1) Notify the CHP Help Desk at HelpDesk@chp.ca.gov or respective Division Network Administrator (DAdmin). The DAdmin will then notify the Department ISO, as well as the appropriate chain of command to initiate the operational recovery process which shall then be coordinated with CCIU.

(2) Notify the owners of lost, stolen, or misplaced unencrypted confidential computer data or “personal information” as required and defined by CIV

1798.29. The Department ISO can provide a sample of the required notification letter to the commander upon request, as well as assist with the notifications to impacted personnel.

(3) Document the loss, theft, or damage of state-owned and state-leased equipment or data, including departmental data stored on personally owned equipment or any other digital media, as required by policy outlined in General Order 100.80, Notification and Report of Emergencies and Unusual Occurrences, and Highway Patrol Manual 11.2, Materials Management Manual, Chapter 8, Equipment.

l. The Department ISO will send the reporting command a SIMM 5340-A to complete and return to the Department ISO within two business days. The Department ISO will review, edit, sign, and submit the SIMM 5340-A to the California Information Security Office within ten business days from the time the incident was reported.

4. INCIDENT RESPONSE. The Computer Incident Response Team (CIRT) is comprised of managers of the Information Management Division (IMD) Network Services Unit, Technical Services Group, Computer Aided Dispatch/Mobile Digital Computer Unit, CCIU, and the Department ISO. The CIRT will respond to, assess, and defuse computer emergencies such as bonafide network breaches, major virus attacks, and system outages, and may assign any other technical resources/staff needed to mitigate incidents. The CIRT can be activated by CIRT members, IMD staff, or the Department ISO, and will utilize departmental incident command system procedures to manage incidents.

THIS PAGE INTENTIONALLY LEFT BLANK

ANNEX A

STATEWIDE INFORMATION MANAGEMENT MANUAL 5340-A, INCIDENT REPORTING AND RESPONSE INSTRUCTIONS

REPORTING CRITERIA (Revised 06/16)

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.

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 noncompliance 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, website 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.

ANNEX A

STATEWIDE INFORMATION MANAGEMENT MANUAL 5340-A, INCIDENT REPORTING AND RESPONSE INSTRUCTIONS *(continued)*

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.**

ANNEX B

GOVERNMENT CODE SECTION 14613.7

14613.**7**. Each state agency that is protected by the Department of the California Highway Patrol, those state agencies currently being protected by contract private security companies, or those state agencies currently under contract with a local governmental law enforcement agency for general law enforcement services, excluding all current mutual aid agreements, shall, as soon as practical, report to the Department of the California Highway Patrol all crimes and criminally caused property damage on state-owned or state-leased property where state employees are discharging their duties. This section shall not apply to incidents that result in the filing of Incidence Memoranda issued by the Parole Divisions of the Department of Corrections and the Department of the Youth Authority.

THIS PAGE INTENTIONALLY LEFT BLANK