California Joint Cyber Incident

Communications and Escalation Framework

California Office of Emergency Services

California Cyber Security Integration Center

Version 1.0 02/24/2018

Table of Contents

Table of Figures and Tables

1. Introduction

A. Audience and Purpose

The purpose of this document is to aide in effective communication and ensure incident information is shared with the appropriate entities in a timely manner to enhance the protective posture during all phases of incident response.

This document provides high level procedural guidance for paths of escalation and coordinated communications during and after a cyber-incident occurs. All entities should incorporate this *Incident Communication Framework* into their local policies and procedures.

B. Key Assertions of incident response

As with all incident response plans, there are many additional external factors stakeholders should consider as they pertain to existing law and / or policy.

- **Incident Ownership remains with the impacted entity.** Regardless of where an incident is referred during its life, ownership of the incident remains with the original, impacted entity. The impacted entity will be the lead response entity with assistance provided as needed or required.
- Reporting a cyber-incident is mandatory for all California State Entities[1] in accordance with State Administrative Manual 5340.4 and Statewide Information Management Manual 5340-A. The current reporting mechanism is the California Compliance and Security Incident Reporting System (Cal-CSIRS).
- Reporting cyber-incidences by non-state entities is NOT mandatory, however it is strongly encouraged. Non-state entities should follow the steps outlined in *Incident Reporting for Non-State Entities* as outlined in section 4 within this document.
- Many federal and California laws require data owners to make timely notification to individuals when their personal information was acquired or reasonably believed to have been required by an unauthorized person, as a result of an information breach. California Civil Code s. 1798.29 and California Civil Code 1798.82 are one example.

2. Overview

To accomplish the objectives delineated in Executive Order B-34-15, the Cal-CSIC has taken a matrixed partnership approach with incidence response. To facilitate this matrixed approach all four of the "core partner" organizations have a full-time presence in the Cal-CSIC; with the Cal-CSIC as the primary coordinating entity charged with ensuring the applicable responsible entity takes the lead in responding to a reported incident based on the context surrounding the incident.

[1] As defined in Government Code Section 11546.1

A. Partnerships

As depicted in Figure 1, the Cal-CSIC serves as the central organizing hub of state government's cybersecurity activities and coordinates information sharing with local, state and federal agencies, tribal governments, utilities and other service providers, academic institutions, and non-governmental organizations. Cal-CSIC is primarily comprised of four core partner organizations: the California Office of Emergency Services (Cal-OES), California Highway Patrol (CHP), California Department of Technology (CDT), and California Military Department (CMD). Each of the four core partners operates within the Cal-CSIC under the umbrella of its specific legal and regulatory authorities during an incident's lifecycle. Key elements which determine which entity gets involved include the type of reporting (victim) organization, the type, scope, and severity of the cyber incident, and whether or not the incident is criminal in nature.

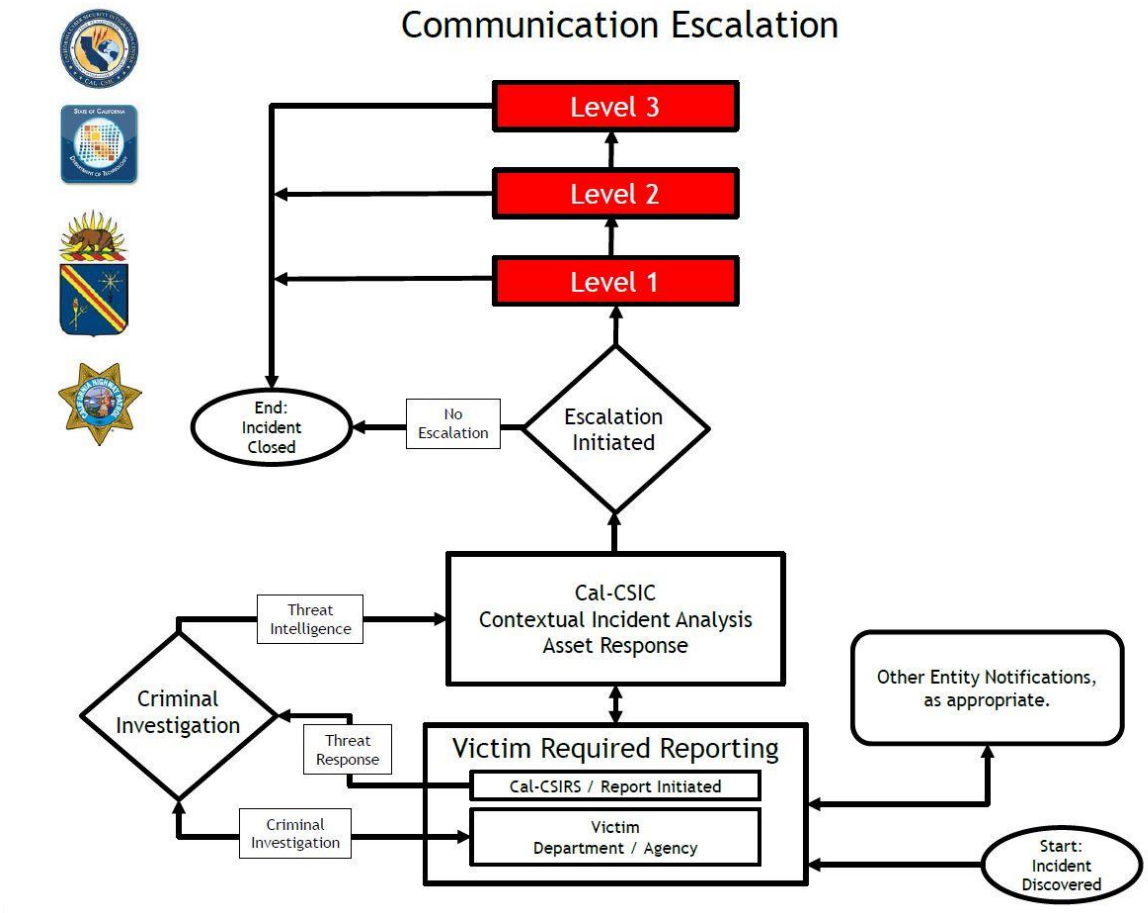

Figure 1 - Incident Reporting Process Flow

This process flow operates under the assumption all incidences are resolved at the lowest possible level, with escalation only when deemed necessary by circumstance. For Executive Branch entities, this process requires the formal submission of all incidents via the California Compliance and Security Incident Reporting System (Cal-CSIRS). Other entities should submit a Cal-CSIC Incident Response Questionnaire (Appendix C) whenever State assistance is required or to inform the Cal-CSIC that an incident has occurred. The system of record for all coordination is the Cal-CSIRS report; which State Executive Branch entities must annotate anytime an action or update surrounding the incident occurs. Cal-CSIRS is accessible to authorized staff of the four core partner agencies for visibility of created, modified and closed incidents to ensure effective coordination.

B. Coordination

The ongoing coordination effort includes communication between the affected / reporting entity and all those assisting the affected / reporting entity with the response. A breakdown or lapse in ongoing communication during the entire life-cycle management of a response may severely hamper the ability to effectively respond to a given cyber incident and may determine how well an agency recovers from an incident. At the onset of any detected or reported incident, the four core engage to assess and determine lead assistance for the incident. In most cases an initial meeting led by affected/reporting entity, and organized and coordinated by Cal-CSIC will take place. This will ensure all parties receive the same information from the onset and the ongoing needs moving forward. Appendix A, Roles and Responsibility by Affected/Reporting Entity Type, illustrate the established coordination protocols.

C. Escalation

The three tiered escalation process is used whenever the four core CAL-CSIC partners determine that a cyber-incident response warrants additional resources or communication with leadership and / or external partners. This escalation process, as seen in Table 1 below, aligns directly with the U.S. Department of Homeland Security (DHS) Cyber Incident Severity Chart, Appendix B. Each tier of escalation has a threshold which should be met in order for the next level to be initiated (seen in the Description column).

California Cyber Incident Severity	Description	Level of Effort Description of Actions
Level 3 (Black)	Poses an imminent threat to the provision of wide-scale critical infrastructure services, State government security, or the lives of California citizens.	Due to its severity, actual or potential impact on public health, welfare, or infrastructure, the Cyber incident requires an extreme amount of State assistance for incident response and recovery efforts, for which the capabilities to support do not exist at any level of State government. Involvement of Public-Private Partnerships if needed for incident.
Level 2 (Red / Orange)	Likely to result in a significant or demonstrable impact to public health or safety, national security, economic security, foreign relations, or civil liberties, or public confidence.	Requires elevated coordination among State Departments, State Agencies, or SLTT governments due to moderate levels and breadth of cyber impact or damage. Involvement of Federal Partners if needed for incident.
Level 1 (Yellow / Green)	May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	Requires coordination among Victim Departments, Victim Agencies, or SLTT governments due to minor to average levels and breadth of cyber related impact or damage. Typically, this is primarily a recovery effort.
Level 0 (White)	Unsubstantiated or inconsequential event.	Steady State, which includes routine watch and warning activities.

Table 1 – California Incident Severity Escalation Matrix

Once Cal-CSIC determines the need to escalate to a new tier CAL-CSIC will work with the affected/reporting entity to initiate a conference call with the four core and other appropriate stakeholders as seen in Tables 2 through 4. It is important to note that at each level of escalation the victim entity (data owner) will be included at the call (with the appropriate level of representation based on the seniority of the others on the call).

Incident Response Coordination	Level 1: Severe Event Conference		
	State CISO	Victim ISO or Impacted SLT Leaders	Victim CIO or Impacted SLT Leaders

Table 2 - Level 1 Coordination

Incident Response Coordination	Level 2: Critical Event Conference			
	State CIO CISO	Victim AISO / ISO or Impacted SLT Senior Leaders	Victim AIO / CIO or Impacted SLT Senior Leaders	Federal Partners

Table 3 - Level 2 Coordination

Incident Response Coordination	Level 3: Catastrophic Event Conference							
	State CIO CISO	Victim AISO / ISO or Impacted SLT Executive Leaders	Victim AIO / CIO or Impacted SLT Executive Leaders	California Government Operations Secretary	Victim Secretary or Impacted SLT Executive Leaders	Federal Partners	Public-Private Partnerships	Governors Office

Table 4 – Level 3 Coordination

- Level 1

Description – May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.

Efforts – Requires coordination among Victim Departments, Victim Agencies, or SLTT governments due to minor to average levels and breadth of cyber related impact or damage. Typically, this is primarily a recovery effort.

- Level – 2

Description – Likely to result in a significant or demonstrable impact to public health or safety, national security, economic security, foreign relations, or civil liberties, or public confidence.

Efforts – Requires elevated coordination among State Departments, State Agencies, or SLTT governments due to moderate levels and breadth of cyber impact or damage; Involvement of Federal Partners if needed for incident.

- Level – 3

Description – Poses an imminent threat to the provision of wide-scale critical infrastructure services, State government security, or the lives of California citizens.

Efforts – Due to its severity, actual or potential impact on public health, welfare, or infrastructure, the Cyber incident requires an extreme amount of State assistance for incident response and recovery efforts, for which the capabilities to support do not exist at any level of State government.

3. Roles and Responsibilities

The following describes the core partners involved in the incident response and their coordination roles:

A. California Cybersecurity Integration Center (Cal-CSIC)

The Cal-CSIC is responsible to:

- Create, review and update all non-state Executive-Branch entity incident reports related to cyber security
- Provide response assistance as needed for **Non-State Executive Branch entities**
- Correspond directly with the non-state Executive Branch entity reporting victim and the CDT SOC when victim entity is a CDT customer (user of .ca.gov domain, CGEN or other CDT services)
- Coordinate with CCIU, CDT SOC and other core partners for key threat indicators
- Develop and coordinate review and approval of threat alerts and critical bulletins with four core partners and CDT SOC
- Provide remediation guidance to victim entities
- Initiate / coordinate discussions with four core partners and CDT-SOC concerning ESF-18 escalation when appropriate
- Ensure the confidentiality, integrity and availability of all information related to the incident

B. California Highway Patrol, Computer Crimes Investigative Unit (CHP-CCIU)

The primary responsibilities of the CHP-CCIU include, but are not limited to:

- Review all Cal-CSIRS submissions for investigative response
- Provide intelligence information which could assist with mitigation or remediation
- Determine if the malicious activity was criminal in nature
- Conduct investigations concerning the criminal activity
- Provide investigative support when requested
- Ensure the confidentiality, integrity and availability of all information related to the incident

C. California Department of Technology (CDT)

a. Office of Information Security (CDT-OIS)

The OIS is responsible to:

- Direct, oversee and track the reporting of incidents by state Executive Branch entities
- Participate as a four core partner through the incident lifecycle
- Direct and advise state Executive Branch entities on privacy issues and privacy breach notification requirements
- Direct and advise state Executive Branch entities on completion of the Cal-CSIRS report
- Review and approve actions in the Cal-CSIR ticketing system to closure
- Ensure root cause analysis and plan of action and milestones (POAM) for remediation are completed for state Executive Branch entities incidents to reduce likelihood or prevent reoccurrence
- Ensure the confidentiality, integrity and availability of all information related to the incident

b. Security Operations Center (CDT-SOC)

The SOC is responsible to:

- Assist with anomaly detection notifications as anomalies are detected, and analysis and triage IF entities are using ca.gov, CGEN or other CDT services
- Coordinate with the Cal-CSIC and CCIU as appropriate
- Correspond directly with CDT customer SLTT entities as appropriate
- Provide remediation guidance to victim entity
- Update or have victim entity update the Cal-CSIRS report as appropriate
- Participate in discussions with CCIU, CMD and Cal-CSIC concerning ESF-18 escalation when appropriate.
- Ensure the confidentiality, integrity and availability of all information related to the incident

D. California Military Department (CMD)

The CMD Computer Network Defense team is responsible to:

- Assist with incident response when requested or required.
- Ensure the confidentiality, integrity and availability of all information related to the incident

E. State Agencies

State Agency Information Security Officers and leaders as appropriately defined are responsible to:

- Ensure entities under their purview are complying with the state incident response reporting policy
- Inform, guide and direct entity security teams to ensure timely and effective response to incidents as appropriate.

F. State Executive Branch Entities

California State Executive Branch Entities shall retain ownership of the incident, comply with state incident reporting and response policy and cooperate fully with entities providing response assistance. These responsibilities include, but may not be limited to:

- Promptly report and respond to incidents
- Provide a single POC for any media/press inquiries
- Provide timely identification of root cause and implementation of corrective actions
- Ensure the confidentiality, integrity and availability of all information related to the incident
- Coordinate with CCIU, Cal-CSIC and CDT as appropriate
- Maintain internal processes to keep agency and leaders well informed.
- Where a State Executive Branch Entity reports to a Cabinet-level Agency, the designated Agency Information Security Officer are responsible to:
    - Ensure entities under their purview are complying with the state incident reporting and response policy
    - Inform, guide and direct entity security teams to ensure timely and effective response to incidents as appropriate

G. Other Entities

All entities, other than defined as California State Executive Branch should:

- Follow all applicable laws and regulations governing the administration of their programs, the Federal Office of Management and Budget (OMB), Federal Information Processing Standards (FIPS) promulgated by National Institute of Standards and Technology (NIST) and any other commercial guidance as required
- Report all incidences to the Cal-CSIC for statewide situational awareness and threat monitoring

4. Incident Reporting Pathways

Reporting an actual or suspected cyber incident begins with the affected entity/organization following the applicable methods listed below. The reporting method will depend on the type of organization reporting the incident.

A. Reporting Protocol for State of California Executive Branch Entities

State Executive Branch entitles shall follow the reporting procedures found in the California Department of Technology (CDT), Office of Information Security (OIS) Incident Reporting and Response Instructions, SIMM 5340A (https://cdt.ca.gov/policy/simm/) and enter the event into the California Compliance and Security Incident Reporting System (Cal-CSIRS) at https://calcsirs.rsam.com. In addition to submitting a Cal-CSIRS incident, State Agencies are encouraged to contact the CHP Computer Crimes Investigation Unit (CCIU) at (916) 450-2200 to initiate an immediate response and ensure the preservation of evidence.

State of California **Executive Branch** Entities requiring immediate assistance outside of regular business hours (8:00am-5:00pm, Monday through Friday) may contact the CHP Emergency Notification and Tactical Alert Center (ENTAC) at (916) 843-4199. The ENTAC will contact CCIU to facilitate immediate assistance.

B. Reporting Protocol for Non-State Executive Branch Entities

All other organizations, including Local, Tribal, Territorial and private sector organizations and entities requesting assistance from the Cal-CSIC should complete the Incident Response Questionnaire (Appendix C) and contact the Cal-CSIC directly at **1-833-REPORT1.** Reporting agencies should then follow up by submitting the associated Incident Response Questionnaire via email to calcsic@caloes.ca.gov.

After-hours calls may be routed to the Cal-OES Duty Officer. Organizations may call the Cal-OES Duty Officer at (916) 845-8911 should the severity of the cyber incident warrant an immediate after-hours response.

5. Initial Response

A. State Executive Branch Entities

State Executive Branch entities will receive an initial response from and communicate with the following:

- **CCIU**: The CCIU determines if the reported incident is criminal in nature. The CCIU will also determine if the threat necessitates escalation at the federal level to agencies such as the Federal Bureau of Investigations (FBI) or the Department of Homeland Security (DHS).
- **CDT OIS**: -The OIS directs, oversee and tracks the reporting of incidents by state Executive Branch entities; participates as a four core partner through the incident lifecycle; direct and advise state Executive Branch entities on privacy issues and privacy breach notification requirements; direct and advise state Executive Branch entities on completion of the Cal-CSIRS report; review and approve actions in the Cal-CSIR ticketing system to closure; ensure root cause analysis and plan of action and milestones (POAM) for remediation are completed for state Executive Branch entities incidents to reduce

likelihood or prevent reoccurrence. Additionally, CDT-OIS may make contact to coordinate information sharing between AISO, ISO and CIOs.

- **CDT SOC**: The CDT SOC assists with anomaly detection notifications as anomalies are detected, and analysis and triage **IF** entity is using ca.gov, CGEN or other CDT services: provides review and inputs for Cal-CSIC joint vulnerability and threat alerts/advisories; coordinates with the Cal-CSIC and CCIU, and corresponds directly with CDT customer (SLTT) entities as appropriate.

B. Other State Government Entities

Other State Branch entities will receive an initial response from and may communicate with the following:

- **CCIU**: The CCIU determines if the reported incident is criminal in nature. The CCIU will also determine if the threat necessitates escalation at the federal level to agencies such as the Federal Bureau of Investigations (FBI) or the Department of Homeland Security (DHS).
- **CDT SOC**: The CDT SOC assists with anomaly detection notifications as anomalies are detected, and analysis and triage **IF** entity is using ca.gov, CGEN or other CDT services: provides review and inputs for Cal-CSIC joint vulnerability and threat alerts/advisories; coordinates with the Cal-CSIC and CCIU, and corresponds directly with CDT customer State, Local, Tribal, and Territorial (SLTT) entities as appropriate
- **CDT OIS**: -The OIS participates as a four core partner through the incident lifecycle and may direct and advise state entities on privacy issues and privacy breach notification requirements Additionally, CDT-OIS may make contact to coordinate information sharing between AISO, ISO and CIOs.
- **Cal-CSIC**: Cal-CSIC may inquire with impacted entity for additional information, particularly when the threat poses a risk to other SLTT government entities within the State of California; threats to Critical Infrastructure or to the public at large.

C. Non-State Government Entities (Local, Tribal, Territory)

- **Cal-CSIC**: Cal-CSIC will coordinate incident response and inquire with impacted entity for additional information, particularly when the threat poses a risk to other SLTT government entities within the State of California; threats to Critical Infrastructure or to the public at large.
- **CCIU**: The CCIU may provide assistance if the incident is criminal in nature. The CCIU will also determine if the threat necessitates escalation at the federal level to agencies such as the Federal Bureau of Investigations (FBI) or the Department of Homeland Security (DHS).
- **CDT SOC**: The CDT SOC assists with anomaly detection notifications as anomalies are detected, and analysis and triage **IF** entity is using ca.gov, CGEN or other CDT services: provides review and inputs for Cal-CSIC joint vulnerability and threat alerts/advisories;

coordinates with the Cal-CSIC and CCIU, and corresponds directly with CDT customer (SLTT) entities as appropriate

- **CDT OIS**: -The OIS participates as a four core partner through the incident lifecycle and may direct and advise state entities on privacy issues and privacy breach notification requirements.

D. All other Organizations and Entities

All other entities will receive a response directly from the Cal-CSIC to triage the incident and coordinate the incident response. The Cal-CSIC will coordinate the response based on the type, scope, and severity of the cyber incident, and whether or not the threat—or California's vulnerability to the threat—is ongoing. Incidents with a possible criminal nature may require further determination in order to understand the level of partner involvement required.

Circumstances surrounding the incident type and characteristics may require coordination with other state, federal, regulatory and / or professional organizations. When external resources are involved, the Cal-CSIC will serve as the central hub for the coordinated effort.

6. Appendices

A. Appendix A – Roles and Responsibilities by Affected/Reporting Entity Type

Refer to California-Joint CICE Framework (Appendix A).pdf

B. Appendix B – Incident Severity Chart

DHS Cyber Incident Severity	California Cyber Incident Severity	Description	Level of Effort Description of Actions
Level 5 Emergency (Black)	Level 3 (Black)	Poses an imminent threat to the provision of wide-scale critical infrastructure services, State government security, or the lives of California citizens.	Due to its severity, actual or potential impact on public health, welfare, or infrastructure, the Cyber incident requires an extreme amount of State assistance for incident response and recovery efforts, for which the capabilities to support do not exist at any level of State government. Involvement of Public-Private Partnerships if needed for incident.
Level 4 Severe (Red) Level 3 High (Orange)	Level 2 (Red / Orange)	Likely to result in a significant or demonstrable impact to public health or safety, national security, economic security, foreign relations, or civil liberties, or public confidence.	Requires elevated coordination among State Departments, State Agencies, or SLTT governments due to moderate levels and breadth of cyber impact or damage. Involvement of Federal Partners if needed for incident.
Level 2 Medium (Yellow) Level 1 Low (Green)	Level 1 (Yellow / Green)	May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	Requires coordination among Victim Departments, Victim Agencies, or SLTT governments due to minor to average levels and breadth of cyber related impact or damage. Typically, this is primarily a recovery effort.
Level 0 (White)	Level 0 (White)	Unsubstantiated or inconsequential event.	Steady State, which includes routine watch and warning activities.

National Cyber Incident Response Plan, December 2016
https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

C. Appendix C – Cal-CSIC Incident Response Questionnaire

California Cyber Security Integration Center

Incident Response Questionnaire

Purpose: The information on this form is collected solely for the purpose of cyber incident reporting to the State of California, specifically by the Cal-CSIC for cyber incident reporting and coordination.

Taken By: _____
Date / Time of Report: _____/_____

Reporting Person / Agency: _____
Name of Person Reporting: _____
Agency / Position: _____

----------INCIDENT SPECIFIC INFORMATION----------

Agency / department: _____ **Type: State Non-State**
Agency Type / Category: _____ **(Circle One)**
(city, county, courts, higher educational, education k-12, other)
Agency address: _____ **Suite:** _____
City: _____ **State:** ____ **Zip:** _____
POC: _____ **Phone:** _____
ISO: _____ **Phone:** _____

Date / Time of Incident: _____/_____ **Date / Time Discovered:** _____/_____

Root Cause of the Incident: _____
(carelessness, inadvertent, intentional, loss, theft, damage)

Description of Incident: _____
_____
_____
_____
_____
_____
_____

Actions taken prior to reporting: _____
_____
_____
_____
_____
_____
_____

Information collected in this form is provided all of the necessary protections and considerations mandated by all applicable Federal and State of California privacy laws.

Version 0.1 **6/15/2017**

D. Appendix D – Contacts

- California Cyber Security Integration Center
  Cal OES
  (916) 636-2997 or
  (833) REPORT1 or (833) 737-6781

- Computer Crimes Investigations Unit
  California Highway Patrol (CHP)
  (916) 450-2200

- Emergency Notification and Tactical Alert Center (ENTAC)
  California Highway Patrol
  (916) 843-4199

- California Security Operations Center
  California Department of Technology
  (916) 228-6144

- California State Chief Information Security Officer (CISO)
  California Department of Technology
  (916) 445-5239