California Joint Cyber Incident Communications and Escalation Framework

California Office of Emergency Services

Version 1.2

07/27/2020

California Cyber Security Integration Center

This page intentionally left blank

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 Response 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-incidents 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.

[1] As defined in Government Code Section 11546.1

2. Overview

To accomplish the objectives delineated in Government Code 8586.5, codifying AB-2813 *California Cybersecurity Integration Center* into state law, the Cal-CSIC has taken a matrixed partnership approach with incidence response. To facilitate this matrixed approach all partner organizations have full-time representation assigned to the Cal-CSIC; with their 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.

A. Partnerships

The Cal-CSIC is comprised of multiple strategic partner agencies, including the California Office of Emergency Services (Cal-OES), California Highway Patrol (CHP), California Department of Technology (CDT), and California Military Department (CMD), the State Threat Assessment Center and regional Fusion Centers that comprise the State Threat Assessment System (STAS); the FBI, DHS, and others as listed in California Government Code § 8586.5. Each of the partner agencies operates within the Cal-CSIC umbrella, but in accordance with their agency's specific legal and regulatory authorities. Key elements which determine which entity gets involved include the reporting (victim) organization, along with the type, scope, and severity of the cyber incident, and whether or not the incident is criminal in nature.

B. Incident Communication Process Flow

As depicted in Figure 1, the Cal-CSIC has the responsibility to serve 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.

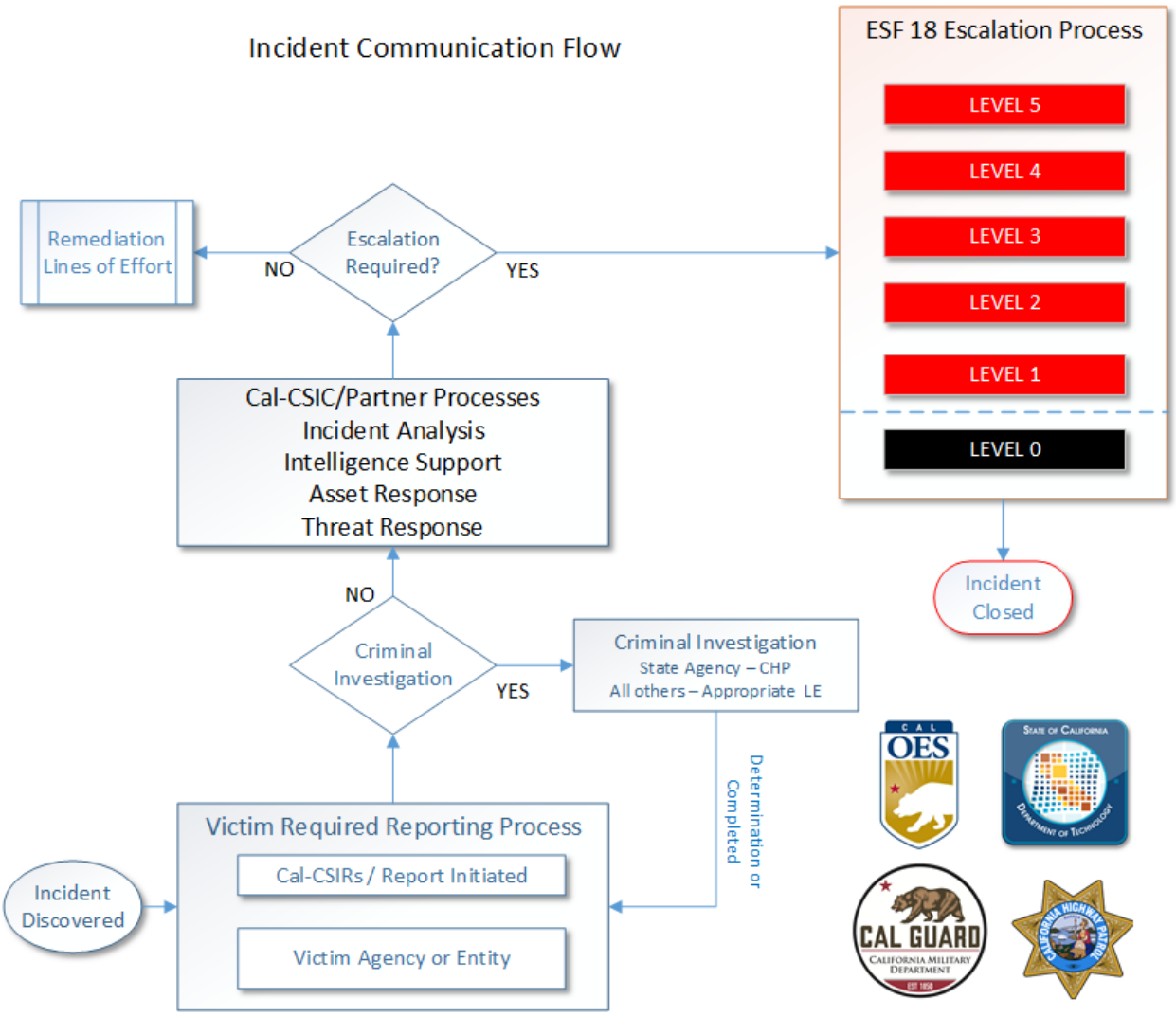

Figure 1 - Incident Reporting Process Flow

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 State Agency and Executive Branch entities, this process requires the formal submission of all incidents via the California Compliance and Security Incident Reporting System (Cal-CSIRS). The system of record for all coordination is the Cal-CSIRS report; which State Agencies or State Executive Branch entities must annotate anytime an action or update surrounding the incident occurs.

Cal-CSIRS is accessible to authorized staff of the Cal-CSIC core partner agencies for visibility of created, modified and closed incidents to ensure effective coordination with state agency events.

Other private sector / non-state entities should either report the incident to their local law enforcement or cybersecurity agency, regional fusion center, or contact the Cal-CSIC directly. The Cal-CSIC will utilize the Cal-CSIC Incident Response Questionnaire (Appendix C) whenever assistance is required or to inform the appropriate entities and agencies that an incident has occurred. The Cal-CSIC will take the report and create an incident ticket within the incident tracking system.

C. Coordination

The ongoing coordination effort includes communication between the affected / reporting entity and all those assisting the affected / reporting entity with the response. At the onset of any detected or reported incident, the incident is reviewed to determine the level of response required. 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.

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
- Communicate with the victim entity directly or via the CDT SOC; ensuring to engage the CDT SOC when victim entity is a CDT user of .ca.gov domain, CGEN or other CDT services.
- Coordinate with CCIU, CDT SOC, CDT Network Protection Team (NPT) and other partners concerning key threat indicators
- Provide threat intelligence analysis and threat analytic support
- Develop, coordinate, review and approve threat alerts and critical bulletins with partners and CDT SOC
- Provide remediation guidance to victim entities
- Initiate / coordinate discussions with 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 Fusion Centers

Fusion Centers in the state have multiple self-defined roles and responsibilities including advising the Cal-CSIC of cybersecurity incidents in their Area of Responsibility for state level visibility and / or when incidents require state level resources. Within this framework, Fusion Center responsibilities include:

- Initial intake of the incident from the private sector
- Educating the victim agency on the incident
- Coordination with local law enforcement and federal entities as applicable
- Coordinating incident response resources to assist the victim through local cybersecurity partnerships or the Cal-CSIC
- Reporting the incident to Cal-CSIC via STAC weekly reports, for awareness and state level reporting
- Timely sharing of indicators of compromise with the Cal-CSIC

C. California Highway Patrol, (CHP-CCIU)

The primary responsibilities of the CHP-CCIU (Computer Crimes Investigative Unit) for State Agencies include, but are not limited to:

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

NOTE: Criminal investigative support for non-State Entities falls under the auspices of local and federal law enforcement agencies as appropriate.

D. California Department of Technology (CDT)

The CDT has multiple branches with various responsibilities concerning incident response and coordination.

1) Office of Information Security (CDT-OIS)

The CDT-OIS has the responsibility to:

- Direct, oversee and track the reporting of incidents by state Executive Branch entities
- Participate as a primary element 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.

2) Network Protection Team (CDT-NPT)

The CDT-NPT is responsible to:

- Provide information concerning movement and data exfil
- Provide "net flow" information for analysis
- Provide network boundary security posture information
- Detect and manages protection rules against malicious activity.

3) Security Operations Center (CDT-SOC)

The CDT-SOC:

- Assists with incident response (threat detection and isolation) when requested or required.
- Assists with anomaly detection notifications as anomalies are detected, and analysis and triage IF entities are using ca.gov, CGEN or other CDT services
- Coordinates with the Cal-CSIC and CCIU as appropriate
- Corresponds directly with CDT customer SLTT entities as appropriate

- Coordinates with Cal-CSIC on remediation approaches
- Coordinates with partner agencies during ESF-18 escalations
- Ensures the confidentiality, integrity and availability of all information related to the incident.

E. California Military Department (CMD)

The CMD Computer Network Defense (CND) team is responsible to:

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

F. State Agencies

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

- Ensure agencies 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.

G. 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.

H. 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 and the entity's internal cyber incident response plan.

A. Reporting Protocol for State of California Agencies

State Agencies 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 and enter the event into the California Compliance and Security Incident Reporting System (Cal-CSIRs). The Cal-CISRs ticket systematically notifies all support agencies, as shown in *Appendix A – State Agency IR Process Flow*.

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 Agencies 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 Entities

All other organizations, including City, County, Local, Tribal, Territorial and private sector organizations and entities have several reporting options available as outlined in *Appendix B – Private Entity IR Process Flow*.

1) Internal Incident Response

Organizations with cyber-insurance should immediately contact their insurance provider for direction and guidance.

2) Fusion Center Reporting

All other organizations, including City, County, Local, Tribal, Territorial and private sector organizations may report the incident directly to their regional Fusion Center, *Appendix F, California Fusion Centers*, or directly to the Cal-CSIC for guidance and coordination support.

3) Cal-CSIC Reporting

Contact the Cal-CSIC directly at **1-833-REPORT1** and be prepared to provide as much detail as possible (See Incident Response Questionnaire at *Appendix C - Cal-CSIC Initial Reporting Questionnaire*). Reporting agencies may choose to complete the Incident Response Questionnaire and submit it to the Cal-CSIC via email to calcsic@caloes.ca.gov.

Calls outside normal duty hours are routed to the Cal-CSIC on-call analyst. If immediate assistance is not available, 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 the Cal-CSIC, which may facilitate communicating with the following:

- **CHP 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 primary element 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.
- **CMD**: The military department provides incident response support, including personnel and equipment augmentation, to the Cal-CSIC as an integral partner agency as defined in government code.

B. Other State Government Entities

Other State Branch entities will receive an initial response from the Cal-CSIC, which may facilitate communicating 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 primary element 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.

- **CMD**: The military department provides incident response support, including personnel and equipment augmentation, to the Cal-CSIC as an integral partner agency as defined in government code.

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

- **Fusion Centers:** Fusion Centers may assume the responsibility of primary incident/event reporting agency for private sector entities based on victim reporting channels. Fusion centers may assist with direct or indirect incident response through local resource coordination and/or requesting Cal-CSIC involvement for incident response.
- **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.
- **Law Enforcement**: The applicable law enforcement entity may provide assistance if the incident is criminal in nature. Law enforcement may 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 corresponds directly with CDT customer (SLTT) entities as appropriate
- **CDT OIS**: -The OIS may participate through the incident lifecycle to direct and advise the Cal-CSIC on privacy issues and privacy breach notification requirements as applicable.
- **CMD**: The military department provides incident response support, including personnel and equipment augmentation, to the Cal-CSIC as an integral partner agency as defined in government code.

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. Escalation / De-Escalation

The five-tiered escalation process is used whenever the Cal-CSIC determines 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 Federal Cyber Incident Severity Chart as well as the ESF-18 (Cybersecurity) Annex to the State Emergency Plan.

The Cal-CSIC leads the ESF-18 effort throughout the incident. During an incident, the Cal-CSIC maintains situational awareness and strategic oversite while the responsibility for tactical response and remediation activities is delegated to the IRT.

The IRT may be comprised of Cal-CSIC agencies, including Federal partner IR capabilities, private sector incident response teams or any combination of thereof to address the four lines of effort shown in Figure 2, and is responsible for carrying out cyber response operations when activated by the ESF-18 Coordination Team. The IRT is responsible for tactical level coordination with other agencies such as law enforcement as well as victim entities, and for communicating with the ESF Coordination Team for situational awareness and strategic level decision-making.

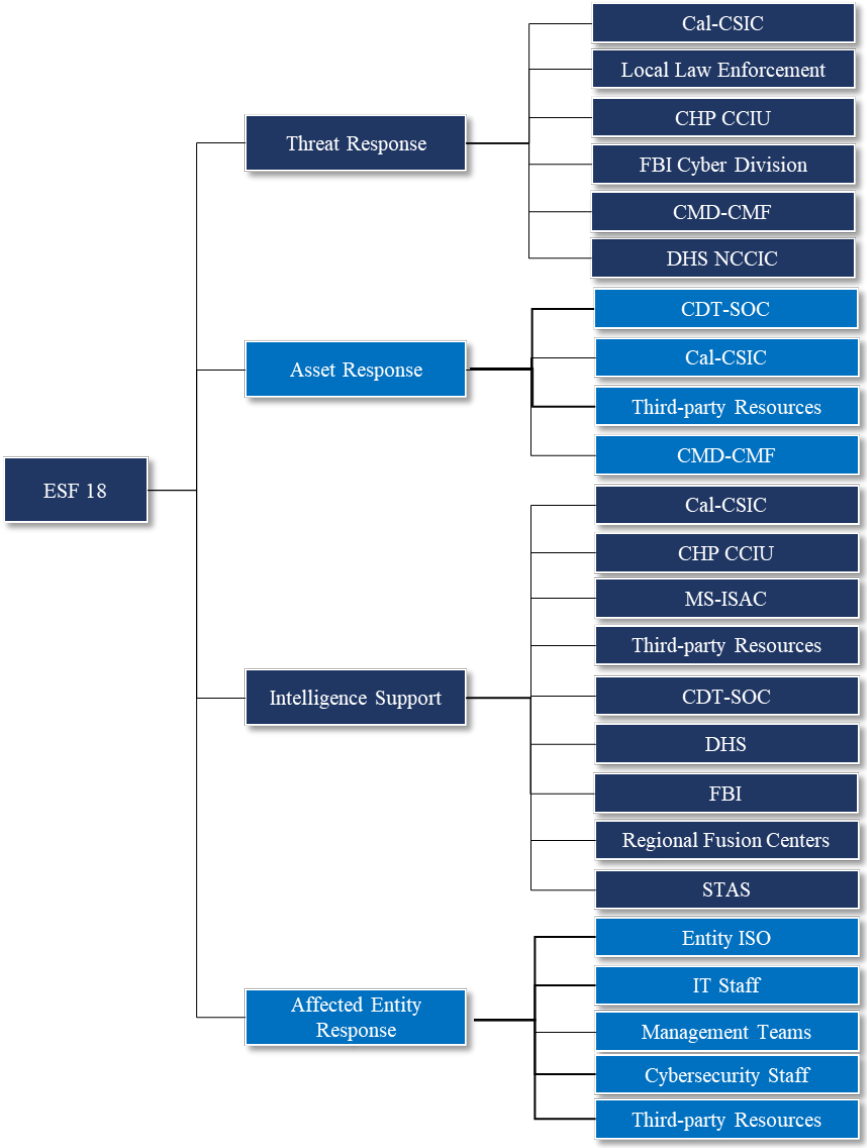

Figure 2 - ESF 18 Lines of Effort

A. Escalation:

Each tier of escalation has a threshold which should be met in order for the next level to be initiated (see Table 1, California Incident Severity Escalation Matrix).

Cyber Incident Severity	Description	Level of Effort Description of Actions
Level 5 Emergency (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)	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 3 High (Orange)	Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	
Level 2 Medium (Yellow)	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 1 Low (Green)	Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	
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, the CAL-CSIC will work with the affected/reporting entity to initiate a conference call with the Cal-CSIC strategic partners and other appropriate stakeholders as seen in Tables 2 through 6. 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).

Cyber Incident Severity	Typical Incident	Coordinating Agencies
Level 1 Low (Green)	Social Engineering Phishing Email	Cal-CSIC staff CDT SOC or non-state affected entity Regional Fusion Center CCIU or law enforcement agency with jurisdiction over the affected entity Other agencies as may be required based on the type and scope of the incident

Table 2 - Level 1 Coordination

1) Level – 1 Low

Coordination – The Cal-CSIC staff will work directly with the victim agency / entity to understand the threat and appropriate actions required. The Cal-CSIC will update leadership the incident. CDT Leadership will allocate resources as required by their internal processes. The Cal-CSIC will coordinate with agencies listed in Table 2, Level 1 Coordination.

Cyber Incident Severity	Typical Incident	Coordination Actions Required
Level 2 Medium (Yellow)	Compromised Accounts O365 exposure / exploitation Phishing with Malware	Cal-CSIC staff CDT SOC or non-state affected entity Regional Fusion Center Possible CDT Strategic Partner Alerting CCIU or law enforcement agency with jurisdiction over the affected entity Other agencies as may be required based on the type and scope of the incident

Table 3 - Level 2 Coordination

2) Level – 2 Medium

Coordination – The Cal-CSIC staff will work directly with the victim agency / entity to understand the threat and appropriate actions required. The Cal-CSIC will update leadership the incident. CDT Leadership will allocate resources as required by their internal processes. The Cal-CSIC will coordinate with agencies listed in Table 2, Level 2 Coordination.

Cyber Incident Severity	Typical Incident	Coordination Actions Required
Level 3 High (Orange)	Single Entity / Agency: Ransomware Attacks Network Centric Attacks - DDoS, TDoS, PDoS	Cal-CSIC Organizational Staff Cal-CSIC Strategic Partner Alerting CCIU / Local LE involvement Regional Fusion Center Involvement FBI Notification Probable Mutual Aid Support Possible STAC Coordination

Table 4 - Level 3 Coordination

3) Level – 3 High

Coordination – The Cal-CSIC staff will work directly with the victim agency / entity to understand the threat and appropriate actions required. The Cal-CSIC will update leadership the incident and begin coordination for supplemental resources as required through the Office of Emergency Services using the Mission Resource Tasking (MRT) process. The Cal-CSIC will coordinate with agencies listed in Table 2, Level 3 Coordination.

Cyber Incident Severity	Typical Incident	Coordination Actions Required
Level 4 Severe (Red)	Large/Multiple Entity / Agency: Ransomware Attacks Network Centric Attacks - DDoS, TDoS, PDoS Temporary Loss of Services Statewide Incident	OES Department of Homeland Security Cal-CSIC Organizational Staff Cal-CSIC Strategic Partner Alerting CCIU / Local LE involvement Regional Fusion Center Involvement FBI Notification / Involvement Probable STAC Involvement Probable FEMA escalation DHS Notification / Involvement Mutual Aid Support Enacted

Table 5 – Level 4 Coordination

4) Level – 4 Severe

Description – The Cal-CSIC will immediately coordinate with the Cal-OES Homeland Security Department Director for direction and notification efforts. Further coordination with national level partners such as FEMA is under the advice and direction of the California HSA on behalf of the Governor's Office. The Cal-CSIC will coordinate with agencies listed in Table 2, Level 4 Coordination.

Efforts – The California HSA, via the Cal-OES HSD Director and Cal-CSIC commander will oversee all coordinated efforts and other ESF functions as required.

Cyber Incident Severity	Typical Incident	Coordination Actions Required
Level 5 Emergency (Black)	Statewide Disaster / Attack Cyber EMP Attack Permanent Loss of Services Incident involving or affecting multiple states / territories	Cal-CSIC Organizational Staff Cal-CSIC Strategic Partner Alerting CCIU / Local LE involvement Regional Fusion Center Involvement STAC Involvement FBI Involvement FEMA Escalation / Involvement DHS Escalation / Involvement Additional Federal and Agency Involvement Mutual Aid Support Enacted

Table 6 - Level 5 Coordination

5) Level – 5 Emergency

Description – All emergency management efforts and activities will require escalated coordination directly with the Cal-OES Homeland Security Advisor, Cal-OES Emergency Management, FEMA, FBI and DHS as required by the event. Further coordination with state level partners such as the STAC and other mutual aid partners is under the advice and direction of the California HSA on behalf of the Governor's Office. The Cal-CSIC will coordinate with agencies listed in Table 2, Level 5 Coordination.

Efforts: National and State level command for Emergency Management is in effect. Activation of other ESF functions are required.

B. De-Escalation:

De-escalation thresholds are outline in ESF-18, section 3, Table 9 – *Escalation and De-Escalation Thresholds*. De-escalation is initiated when the steady state of the incident returns to the level of the next lower applicable level.

7. Appendices

A. Appendix A – State Agency IR Process Flow

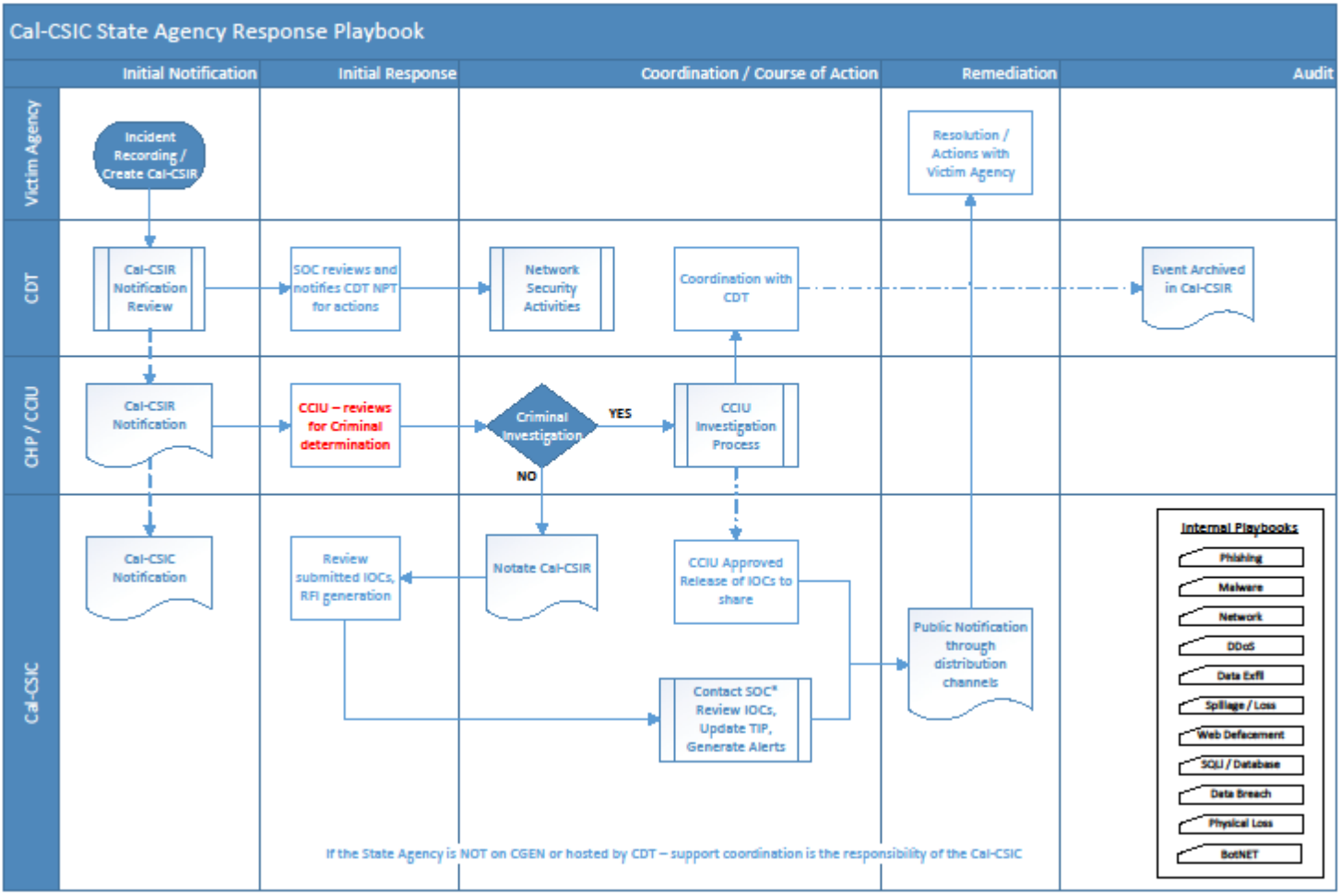

Figure 3 - State Agency IR Process Flow

B. Appendix B – Private Entity IR Process Flow

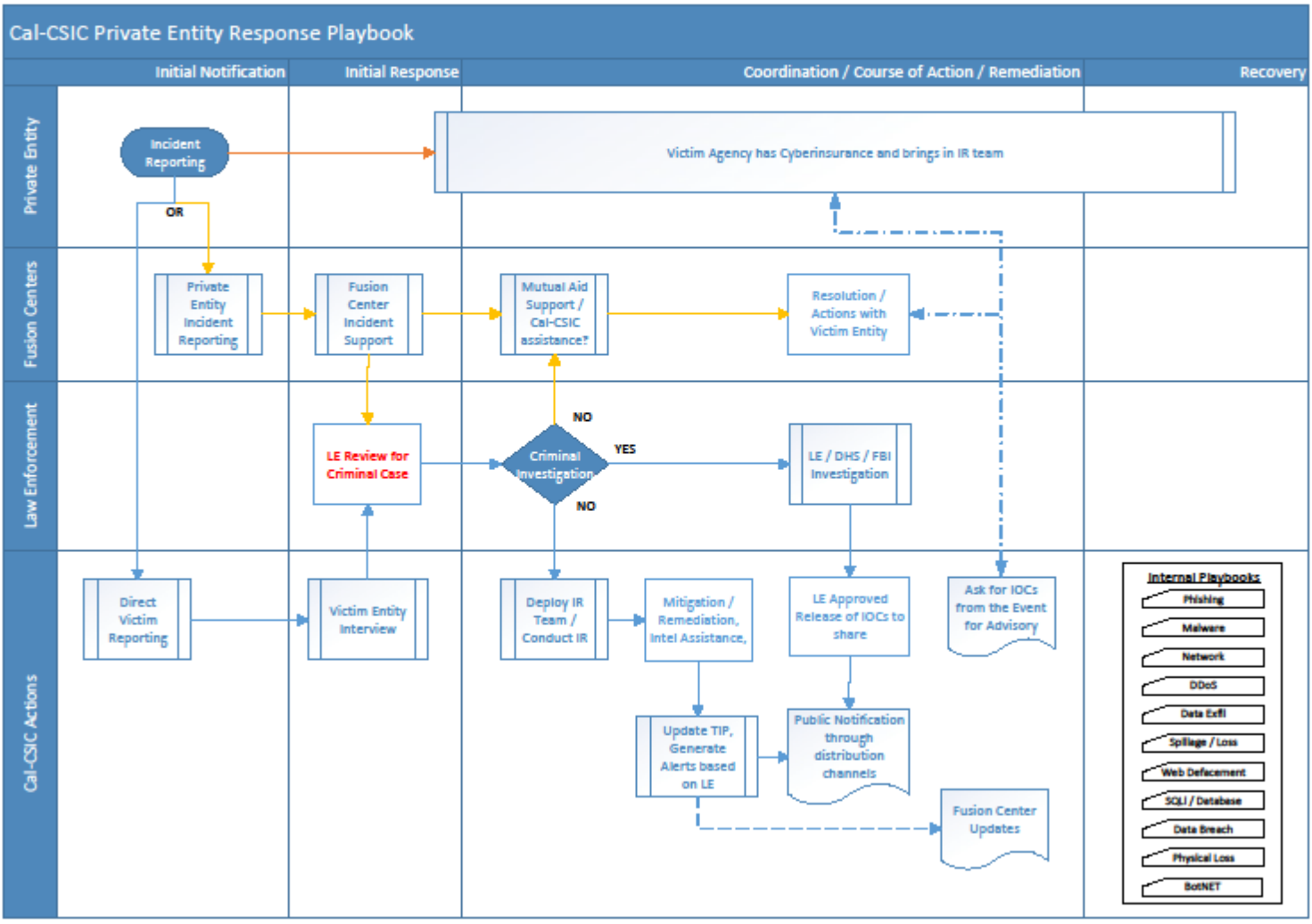

Figure 4 - Private Entity IR Process Flow

C. Appendix C – PPD 41 Cyber Incident Severity / National Response Coordination Crosswalk Chart

Description	DHS Disaster Level	PPD 41 Cyber Incident Severity	Description	Actions
Due to its severity, size, location, actual or potential impact on public health, welfare, and infrastructure it requires an extreme amount of federal assistance for response and recovery efforts for which the capabilities to support do not exist at any level of government.	Level 1	Level 5 Emergency (Black)	Poses an imminent threat to the provision of wide-scale critical infrastructure services, national government security, or the lives of US citizens.	Effect
Requires elevated coordination among federal and SLTT governments due to moderate levels and breadth of damage. Significant involvement of FEMA and other federal agencies.	Level 2	Level 4 Severe (Red)	Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties	Presence
		Level 3 High (Orange)	Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	
Requires coordination among federal and SLTT governments due to minor to average levels and breadth of damage. Typically, this is primarily a recovery effort with minimal response requirements.	Level 3	Level 2 Medium (Yellow)	May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	Engagement
		Level 1 Low (Green)	Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	
No event or incident anticipated. This includes routine watch and warning activities.	Level 4	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

D. Appendix D – Initial Response Victim Questionnaire

UNCLASSIFIED//FOR OFFICIAL USE ONLY

California Cybersecurity Integration Center

Incident Response Victim Questionnaire

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Version 1.0 November 19, 2019

E. Appendix E – Cal-CSIC Initial Reporting Questionnaire

California Cyber Security Integration Center

Initial Report 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, higher educational, education k-12, etc.)
Agency address: _____ Suite: _____
City: _____ State: ____ Zip: _____
POC: _____ Phone: _____
ISO: _____ Phone: _____

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

Incident Classification: _____ Severity Category (Level – 1 2 3) _____
(degradation, outage, theft, loss, etc.) (See comm plan for severity / category)

Root Cause of the Incident: _____
(inadvertent activity, theft, DDOS, malware, virus, hacking, phishing, etc.)

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 1.3 11/20/2019

F. Appendix F - California Fusion Centers

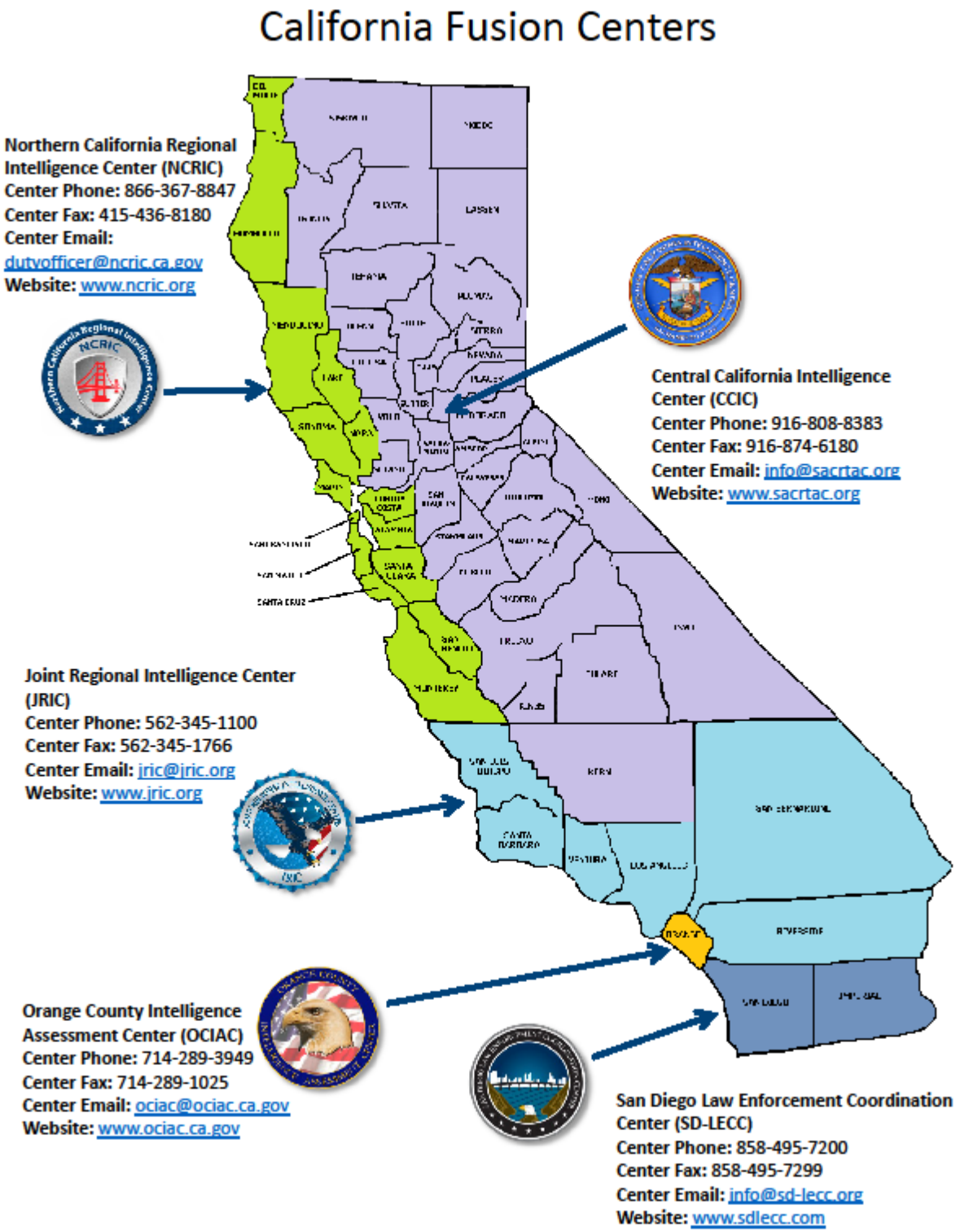

Figure 5 - California Fusion Centers

G. Appendix G – Contacts

- California Cyber Security Integration Center
  Cal OES
  (916) 636-2997
  (833) REPORT-1 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