California Emergency Support Function 18

Cybersecurity

Annex to the California State Emergency Plan

Lead Agency:

California Governor's Office of Emergency Services

Cybersecurity
CA-ESF 18

January 2020

Table of Contents

Emergency Function Agencies/Departments

Table 1: Emergency Function Agencies/Departments[1]

Cybersecurity Lead Agencies/Departments
Lead Agency
California Governor's Office of Emergency Services (Cal OES)
Primary Agencies/Departments
California Department of Technology (CDT)
California Highway Patrol (CHP)
California Military Department (CMD)
California Department of Justice (CA-DOJ)

[1] See **Table 8** for a list of Supporting Agencies/Departments.

Section 1
Introduction

Introduction[2]

Cyber threats to California's security are increasing in frequency, scale, sophistication, and severity. The ranges of cyber threat actors, methods of attack, targeted systems, and victims are also expanding. The United States (U.S.) government's 2018 assessment of the threat environment concluded that the potential for surprise in the cyber realm will increase in the coming years, as more devices are connected to the internet and threat actors grow their attack capabilities. Attack methods such as ransomware and malware have spread globally and are capable of disrupting operations and exposing sensitive data to vulnerability.

Cybercrime is estimated to cause in excess of $300 billion annually in global damages and losses, and the U.S. intelligence community remains concerned by the increasingly damaging impacts of cyber-attacks. California has a wide variety of Internet-related businesses, both in the development cycle and the e-commerce sector, making the state an attractive target for cybercriminals. Cybercriminals also target personal information stored online for use in fraudulent activities. Healthcare, financial institutions and e-commerce are typical targets of criminal data breaches of personal information.

California is home to several Academic Centers of Excellence[3], military technology firms, defense industrial base companies, cutting-edge technology companies, and research facilities—all attractive targets for nation-states or potential adversaries who may be seeking to target the United States with a cyber-attack. California represents the fifth largest economy in the world and possesses nearly 232,000 state employees. With a majority of breaches still beginning with errant email clicks by users, California's state infrastructure faces internal risk as well.

Though a large-scale cyber-attack has not been observed in the U.S., it remains a possibility because malicious cyber actors, terrorist groups and their supporters, and nation-states have demonstrated both an interest in and the ability to disrupt their adversaries' cyber infrastructure. California has a high number of Internet-facing

[2] State of California Emergency Plan (SEP). October 2017. [Pg. 18]
Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community. February 2018.
National Cyber Strategy. September 2018.
[3] Academic Centers of Excellence are a statewide network of higher education institutions that partner with business and industry to provide subject matter expertise, research, and educational resources on a given area.

industrial control networks which operate and regulate critical infrastructure including oil facilities, electricity, and Internet backbone lines. A cyber-attack on any of these or on the emergency services sector could cause severe disruption and loss of life.

Emergency Support Function (ESF) 18 coordinates resources to prepare, mitigate, respond, and recover from a significant cybersecurity event.

Purpose / Mission / Goals

The purpose of this Annex is to define CA-ESF 18 actions and roles for stakeholders of all ESFs during preparedness, mitigation, response, and recovery. The purpose and mission of CA-ESF 18 is to coordinate for cyber critical response including the detection, mitigation, and information sharing related to statewide cyber-related events.

This Annex will facilitate, coordinate, and support the following core functions of the ESF:

- Refining inter-agency and cross-sector information coordination, encouraging information sharing, and performing threat analysis;
- Sharing information in a way that protects privacy, confidentiality, and civil liberties;
- Establishing and maintaining the Incident Response Team (IRT) to detect, report, and respond to cyber incidents; and
- Developing a statewide cybersecurity strategy which advances California's cyber capabilities.

Scope

The CA-ESF 18 Annex describes the organizational framework for support and coordination among the CA-ESF 18 stakeholders. Stakeholders within CA-ESF 18 will use this framework as a basis for cyber incident coordination including cyber terrorism, cyber incidents involving critical infrastructure information systems, technological emergencies, or other emergencies or disasters with impacts on information technology (IT) capabilities or secure data and privacy information in the State of California.

The Annex provides an organizational structure and assignment of responsibilities, concept of CA-ESF 18 coordination, annex maintenance information, and operational tools to support operations of the ESF. The Annex will be the base guidance for CA-ESF 18 stakeholders and their operations before, during, and after an incident with implications related to cybersecurity.

CA-ESF 18 stakeholders coordinate in accordance with relevant statutory and regulatory authorities during all phases of emergency management. CA-ESF 18 stakeholders coordinate with state and local departments and agencies during

response, but do not supersede the authority of these entities. CA-ESF 18 and relevant state and local entities work together to protect life and property in the State of California.

The State Operations Center (SOC) and the California Cybersecurity Integration Center (Cal-CSIC) are essential entities in cyber incidents, and their roles are integrated in the coordination structure of CA-ESF 18. The SOC, under the management of Cal OES, oversees federal resource requests and resolves regional-level priority issues. Cal-CSIC, also managed by Cal OES, provides cybersecurity information integration, threat analysis, and response and recovery coordination for the state through the partnership of Cal OES, CDT, CHP, and CMD. SOC and Cal-CSIC are both organized in accordance with the Standardized Emergency Management System (SEMS), which instates a standard organizational structure and terminology among emergency management agencies in California and integrates and standardizes key elements of the emergency management system in the state.

Cyber incidents vary in scale and severity, and CA-ESF 18 stakeholders will need to respond in proportion to the threat to effectively manage resources and personnel. **Table 2** describes the incident severity scale to be used by CA-ESF 18, including the level of effort and expected coordination with state, local, tribal, and territorial (SLTT) governments and other mission partners.

Table 2: Cyber Incident Severity Matrix

California Cyber Incident Severity	Description	Level of Effort—Description of Actions
Level 0—Steady State	Unsubstantiated or inconsequential event.	Steady State, which includes routine watch and warning activities.
Level 1—Low	Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	Requires coordination among State Departments 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 2—Medium	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 3—High	Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	Requires elevated coordination among State Departments, State Agencies, or SLTT governments due to moderate levels and breadth of damage. Potential involvement of FEMA and other federal agencies.
Level 4—Severe	Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.	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 5—Emergency	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, size, location, 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.

Interactions with Other Emergency Support Functions

CA-ESF 18 interacts and coordinates with other state emergency support functions to perform the core functions of CA-ESF 18 and other ESFs as requested. CA-ESF 18 has significant cross-cutting interactions with the ESFs listed in **Table 3**.

Table 3: Emergency Support Function Interactions

Emergency Support Function	Interaction
CA-ESF 1—Transportation	– Provide status of all primary and alternate cyber controls and components in Transportation affected by, or affecting response to, cyber incidents – Coordinate during cyber incidents impacting traffic monitoring systems, industrial control systems, and geographic information systems (GIS) – Conduct global positioning system (GPS) tracking and monitoring of sensitive cargo, such as radiological materials or railway fuels
CA-ESF 2—Communications	– Provide status of all primary and alternate communications affected by, or affecting response to, cyber incidents – Provide alternate communications during potential cyber incidents impacting GIS and digital communications
CA-ESF 5—Management	– Provide over-arching ESF coordination with the Regional Emergency Operations Centers (REOCs)/SOC, Joint Field Office (JFO), and other emergency functions – Coordinate during cyber incidents impacting GIS, the Web Emergency Operations Center ("WebEOC") system, and other forms of response technology – Coordinate the collection of status information for all technology-based systems, devices, and connections affected by, or affecting the response to, a cyber incident – Provide state and local leadership with current status of all technology-based systems, devices, and connections consistently throughout a cyber incident
CA-ESF 7—Resources	– Provide alternate data processing repositories, cloud site(s), and incident reporting to facilitate and support successful data processing from an alternate location during a cyber-event – Coordinate during cyber incidents impacting industrial control systems

Emergency Support Function	Interaction
CA-ESF 8—Public Health and Medical	– Coordinate during cyber incidents impacting public health and medical functions including, but not limited to, emergency management, healthcare facility durable equipment/infrastructure, food/drug, and radiological/nuclear systems
CA-ESF 10—Hazardous Materials	– Coordinate during cyber incidents impacting the equipment that monitors and releases hazardous materials, controlled by industrial control systems
CA-ESF 11—Food and Agriculture	– Coordinate during cyber incidents impacting manufacturing equipment and other industrial control systems used in Food and Agriculture
CA-ESF 12—Utilities	– Coordinate during cyber incidents impacting industrial control systems that support critical infrastructure
CA-ESF 13—Law Enforcement	– Coordinate investigation, forensics, and arrest related to cyber incidents – Request federal assistance when needed
CA-ESF 14—Recovery	– Recovery from a cyber incident and the restoration of critical functions and operations – Coordinate with Federal entities and partners to provide expanded and enhanced cyber response and recovery capabilities
CA-ESF 15—Public Information	– Coordinate the content and release of security notifications to the public and receiving information from Public Information Officers through Cal OES Office of Crisis Communications and Media Relations and Technology Agency's Public Information Officer
CA-ESF 17—Volunteer and Donations Management	– Coordinate to provide volunteers to assist with response to cyber-attacks as needed

Authorities and References

Authorities and references refer to those documents, plans, guidance, policies, and laws that inform and regulate this Annex. Authorities provide an overview of the codes, statutes, ordinances, executive orders, regulations, and formal agreements that are relevant to CA-ESF 18 stakeholders and the guidance included in this Annex. References are the documents and other publications utilized for the creation, update, and maintenance of this Annex. **Table 4** provides a high-level overview of key state, federal, and other authorities and references that have informed the development of this Annex.

Table 4: Authorities and References

Authorities and References	
State	
California Government Code Section 8586.5 (2018)	Assembly Bill 2813 added section 8586.5 to the California Government Code, which codified Cal-CSIC in state law. Cal-CSIC was originally the result of Executive Order B-34-15. This government code re-establishes this order as part of California state law.
California Government Code Section 8558 (2018)	Senate Bill 532 amended Section 8558 of the Government Code to include cyberterrorism in the conditions that constitute a state of emergency and local emergency.
Joint Cyber Incident Response Guide (2018)	The Joint Cyber Incident Response Guide (JCIRG) provides guidance for governmental and non-governmental entities within California developing incident response plans (IRPs). CA-ESF 18 works with existing local and regional IRPs that are based on the guidance provided in this document. JCIRG includes information on legal reporting requirements at the state and federal levels. As an incident escalates, these reporting requirements should be followed and met to ensure legal compliance.
State of California Hazard Mitigation Plan (2018)	The State of California Hazard Mitigation Plan (SHMP) includes a hazard profile on cyber threats, which describes in detail the threats California faces from cyber incidents, existing mitigation measures against losses from cyber incidents, and potential new mitigation projects to defend against cyber incidents. The SHMP describes the potential and historical impacts of a cyber incident, and highlights Cal-CSIC's role in encouraging private-public partnerships.

Authorities and References	
Federal	
Presidential Policy Directive (PPD) 41 (2016)	PPD 41 is a directive signed under the Obama administration which highlights the importance of cybersecurity to national security and establishes a system for federal-level cyber incident coordination. The PPD establishes lead Federal agencies for significant cyber incidents and requires the Departments of Justice and Homeland Security to provide updated contact information to the public for reporting purposes.
National Cyber Incident Response Plan (NCIRP) (2016)	The NCIRP serves as the cyber annex to the Federal Interagency Operation Plan and describes the national approach for cyber incident management. The NCIRP describes the roles of the private sector as well as local, state, and federal agencies in cyber response, built from the guidance provided in PPD 41 and the National Cybersecurity Protection Act of 2014.
National Cybersecurity Protection Act of 2014	The National Cybersecurity Protection Act of 2014 codified the National Cybersecurity and Communications and Integration Center, which is similar in function to Cal-CSIC, and coordinates information among federal agencies, state and local governments, and the private sector.
National Institute of Standards and Technology (NIST) 800-53 (2013) and 800-61(2008)	NIST Special Publications 800-53 and 800-61 provide recommendations and guidance for federal-level cyber incident management. 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, provides a menu of recommended controls for protecting organizational operations and assets against cyber threats. 800-61, the Computer Security Incident Handling Guide, provides operations response guidance for computer security incidents, including information on building response capabilities, analyzing incident data, and determining the level of response required by an incident.
Joint Publication 3-28: Defense Support of Civil Authorities (2018)	Joint Publication 3-28 is a document from the Joint Chiefs of Staff which sets forth a doctrine for planning, conducting, and assessing defense support of civil authorities. The publication includes changes that authorize the use of federal cyber assets in defense operations and describe defense support for cybersecurity activities.

Authorities and References	
Other	
National Association of State Chief Information Officers (NASCIO) Cyber Disruption Response Planning Guide (2016)	The NASCIO Cyber Disruption Planning Guide provide guidance for states developing cyber disruption plans. Included in this guidance is information on how to provide planning for governance, risk management, communication, and training. The Guide also includes recommendations and operational tools to assist states in developing plans.

Relationship to Other Plans

This Annex interacts with other relevant documents, guidance, and plans. This section provides information on how this Annex interacts with other state and regional documents, and how this document is intended to be used in relation to these other plans. This Annex is not intended to replace existing documentation, but rather supplement them or provide a different scope of planning that creates a fuller picture of cybersecurity emergency operations for use by planners and response and recovery partners.

Table 5: Plan Relationships

Annex Relationship to Other Plans	
State	
California Joint Cyber Incident Response Guide (2018)	The JCIRG provides tactical guidance on response operations for governmental and non-governmental entities within California. This Annex builds from information provided in the JCIRG, but provides higher-level, more overarching guidance and information, and is directed toward CA-ESF 18.
California Joint Cyber Incident Communications and Escalation Framework (2018)	The California Joint Cyber Incident Communications and Escalation Framework (CICE) provides high level procedural guidance for paths of escalation and coordinated communications during and after a cyber-incident occurs. Similar to the interaction between the JCIRG and this Annex, this Annex builds from and supplements the information provided in the CICE, providing overarching guidance related to operations, whereas the information provided in the CICE is more specific and targeted toward communications and escalation practices.

Annex Relationship to Other Plans	
State of California Emergency Plan (2017)	The State of California Emergency Plan (SEP) is the base plan to which this document is an annex. This Annex provides additional guidance related to CA-ESF 18 that supplements the more general information provided by the SEP.
State of California Continuity Planning Guidance (2018)	The State of California provides guidance for local and county entities within the state developing continuity plans. This guidance is broadly applicable to continuity after any hazard but can be applied to cybersecurity. The guidance includes considerations for redundancy and continuity in communications and information technology that are relevant to cybersecurity planning and operations.
Other	
State of California Catastrophic Incident Base Plan (2008)	The State of California and entities within California have developed several catastrophic plans which provide guidance for high-impact events such as earthquakes and flooding. The information provided in these catastrophic plans are relevant to cyber planning and CA-ESF 18 as catastrophes would be likely to impact cyber infrastructure or other cybersecurity assets. These plans should be considered alongside this Annex when managing cyber response for a catastrophic event.
Northern California Catastrophic Flood Response Plan (NCCFRP) (2018)	
Bay Area Earthquake Plan (2016)	
Cascadia Subduction Zone- Earthquake and Tsunami Response Plan (2013)	
Southern California Catastrophic Earthquake Response Plan (2010)	

Section 2

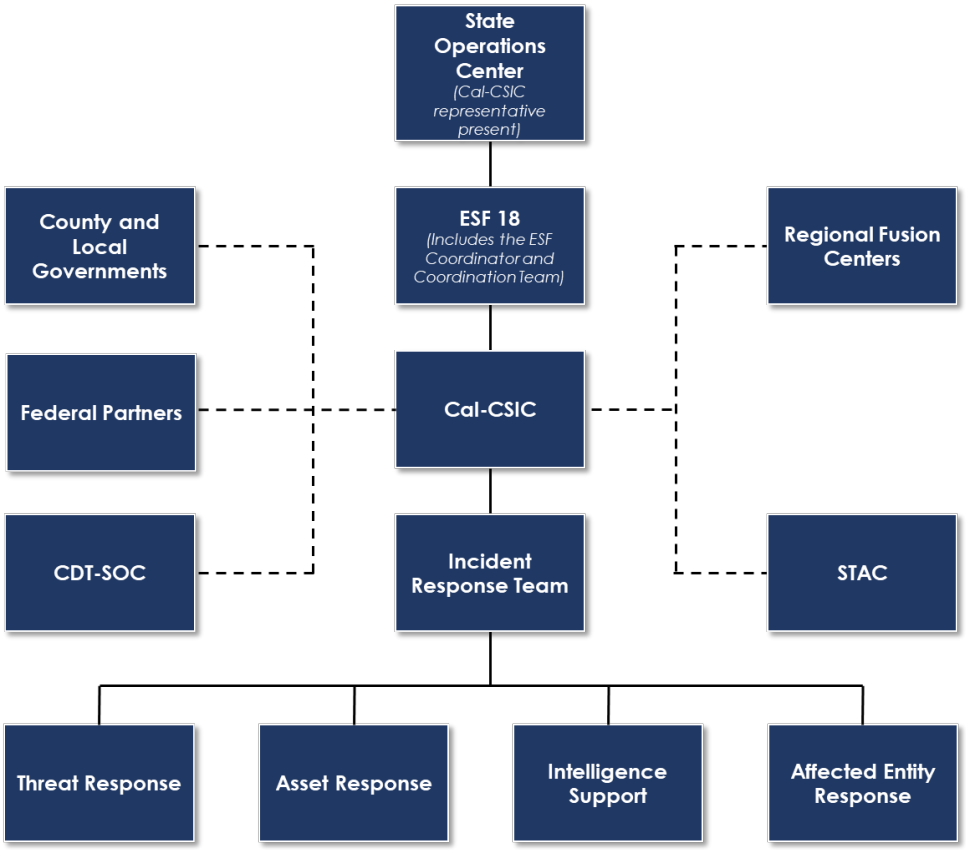
Organization and Assignment of Responsibilities

Organization

The CA-ESF 18 coordination team consists of an alliance of state agencies, departments, and other stakeholders with similar functional responsibilities which collaboratively mitigate against, prepare for, respond to, and recover from emergencies within the emergency management system in California. The organization of CA-ESF 18 is consistent with all 18 emergency support functions to provide common language and standardized organizational concepts. Core functions are used to group similar capabilities in categories of services and support. An ESF may have several core functions, capabilities, and categories of services and support.

The CA-ESF 18 team coordinates with local, regional, state, and federal partners within the established organizational structure and within lines of effort to carry out core functions. This includes coordination with regional fusion centers (RFCs), the state response support structure (including the SOC), and the federal support structure. Coordination among these entities is essential for effective and unified response operations. **Figure 1** shows the organizational structure within CA-ESF 18, and in coordination with other entities. This figure is not reflective of specific reporting pathways, but rather represents the overall internal organizational structure of CA-ESF 18.

Figure 1: CA-ESF 18 Organizational Structure



Emergency Function Administration Structure

Cal OES, through Cal-CSIC, is assigned to lead CA-ESF 18 based on its authorities, resources, and capabilities. Though Cal OES is officially designated as the Lead Agency for the development, implementation, and maintenance of the CA-ESF 18 Annex, these duties are to be performed through Cal-CSIC, an entity of Cal OES. To provide clarity around Cal OES's role as a member of the state's cyber response body and as the state's overall emergency response coordinator, this document will refer to the Lead Agency as Cal OES when describing cyber-focused response operations. References to Cal OES will describe the entity's role in non-cyber-focused response operations, such as consequence management, resource coordination, and core emergency management-related activities. Therefore, Cal OES's responsibilities as the Lead Agency include:

- Overseeing the development, implementation, and maintenance of the CA-ESF 18 Annex

- Providing guidance and direction to the IRT
- Setting multi-year goals and objectives as part of the state cybersecurity strategy
- Fostering participation and jurisdictional commitment to the identified strategy
- Reviewing and arbitrating issues within the ESF in coordination with the identified Lead entity within Cal-CSIC or affected entity if the issue involves a specific cyber incident
- Monitoring the IRT and other CA-ESF 18 stakeholders to ensure compliance and completion of assigned tasks

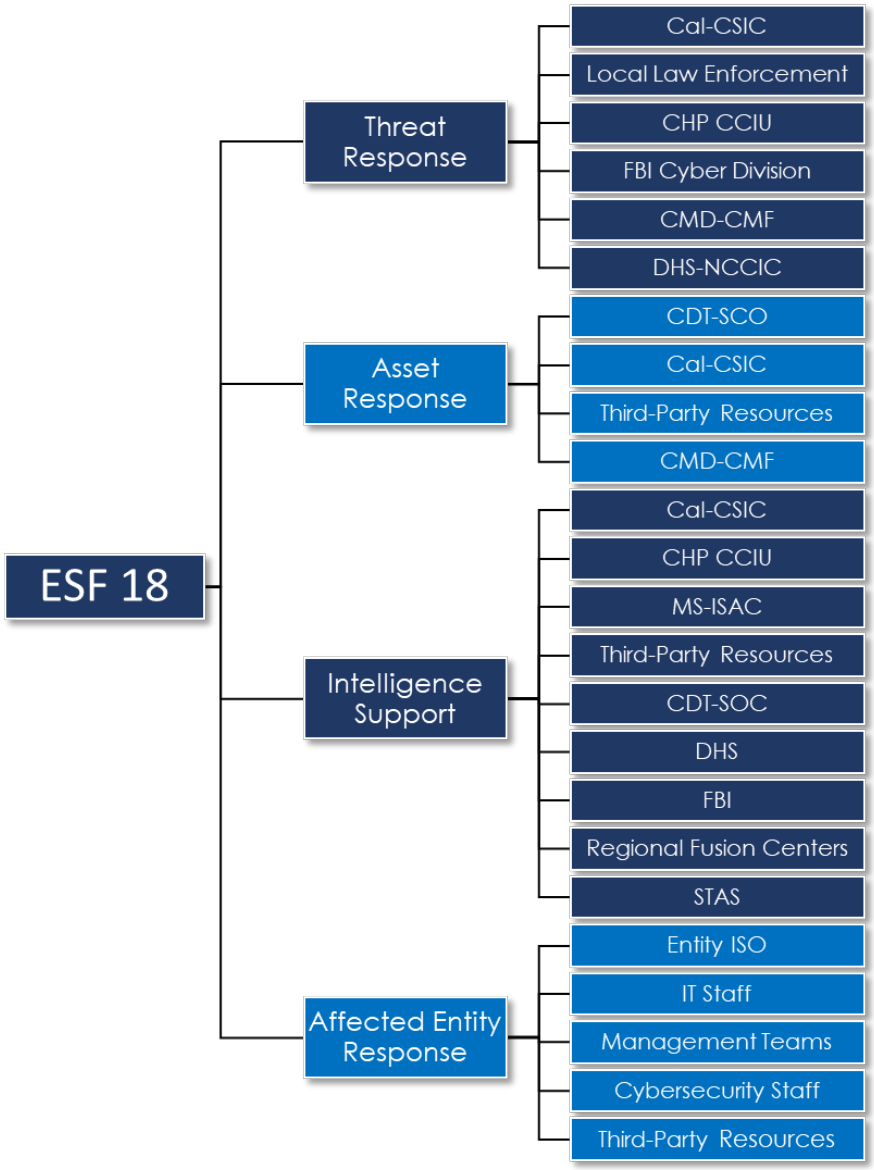
Lines of Effort

Cyber incident management under CA-ESF 18 is categorized in four lines of effort, which identify core needs during a cyber incident and implement the core functions of CA-ESF 18. These four lines of effort are Threat Response, Asset Response, Intelligence Support, and Affected Entity Response. Definitions for these lines of effort can be found in **Table** 10. The entities and partners listed in **Table 6** and **Figure 2** may be enlisted to support cyber incident response operations within each of the lines of effort. For more information on lines of effort, see **Attachment C**.

Table 6: Lines of Effort and Possible Participating Entities

Line of Effort	Possible Participating Entities
Threat Response	**Local:** – Local law enforcement **State:** – Cal-CSIC – CHP Computer Crimes Investigation Unit (CHP-CCIU) – CMD-CMF **Federal:** – Federal Bureau of Investigation (FBI) Cyber Division – Department of Homeland Security National Cybersecurity and Communications Integration Center (DHS NCCIC)
Asset Response	**State:** – CDT State Operations Center (CDT-SOC) – Cal-CSIC – CMD-CMF **Private Sector:** – Third-party cybersecurity resources
Intelligence Support	**State:** – Cal-CSIC – CDT-SOC – CHP CCIU **Federal:** – Multi-State Information Sharing and Analysis Center (MS-ISAC) – Department of Homeland Security (DHS) – FBI **Regional:** – RFCs **Local:** – State Threat Assessment System (STAS) **Private Sector:** – Third-party cybersecurity resources
Affected Entity Response	**Local:** – Entity Information Security Officer (ISO) – IT staff – Management teams – Cybersecurity staff **Private Sector:** – Third-party cybersecurity resources

Figure 2: ESF Lines of Effort Organization



Decision-Making Process

Due to the many stakeholders, agencies, and levels of government involved in the organizational structure associated with CA-ESF 18, decision-making procedures have been established to ensure effectiveness and efficiency.

When an incident occurs, Cal-CSIC will coordinate with the affected entity as part of a unified command structure. Cal-CSIC will work directly with the affected entity to guide

response efforts and direct additional support and resources as needed. This unified command structure will form the central authority for decision-making.

Cal-CSIC assumes a leading role in decision-making while achieving consensus between CA-ESF 18 stakeholders and supporting the needs of the affected entity. The role of the affected entity is central to the response process and should not be superseded by Cal-CSIC or any other entity within CA-ESF 18 for as long as it is feasible to do so. Affected entities may receive assistance from CA-ESF 18 as needed.

To provide overarching support to the affected entity, the remainder of Cal-CSIC and CA-ESF 18 will coordinate to make decisions based on the direction, vision, and needs identified by the affected entity. These decisions include resource allocations, need for escalation, and communications considerations.

The IRT reports to Cal-CSIC and performs tasks as mandated by Cal-CSIC, CA-ESF 18, and the affected entity, and refers directly to Cal-CSIC for any decision-making needs.

Lead Agency

Cal OES is responsible for the management oversight of CA-ESF 18. Cal OES is assigned to lead CA-ESF 18 based upon its authorities, resources, and capabilities in the State of California Emergency Plan and has ongoing responsibilities throughout the preparedness, mitigation, response, and recovery phases of emergency management. As the Lead Agency for CA-ESF 18, Cal OES provides ongoing communication, coordination, and oversight for CA-ESF 18 throughout all phases of emergency management.

CA-ESF 18 Coordination Team: Cal-CSIC

Cal-CSIC is responsible for overseeing the development, implementation, and maintenance of the CA-ESF 18 Annex. Cal-CSIC will provide ongoing communication, and coordination for CA-ESF 18 throughout all phases of emergency management. However, during response operations, primary responsibility for implementing tactical activities and remediation will transition to the IRT, while Cal-CSIC will maintain situational awareness and strategic oversight of the incident.

Cal-CSIC is primarily comprised of four strategic partner organizations: Cal OES, CHP, CDT, and CMD. Each of the four partners operates within Cal-CSIC under the umbrella of its specific legal and regulatory authorities during an incident's lifecycle. Key elements determine which entity will be involved in cyber response, such as:

- Type of reporting (victim) organization
- Type of cyber incident

- Scope of cyber incident
- Severity of cyber incident
- Whether the cyber incident is criminal in nature

At the onset of any incident, the Cal-CSIC will engage to assess and determine lead assistance for the incident. In most cases, an initial meeting led by the affected entity and Cal-CSIC will take place to activate and determine the makeup of the IRT.

CA-ESF 18 Coordinator

Each ESF in the State of California has a coordinator role to provide information and coordination between the broader response community and the emergency support function stakeholders. The CA-ESF 18 Coordinator facilitates coordination, cooperation, and unity of operations among CA-ESF 18 stakeholders. The CA-ESF 18 Coordinator will sit at and provide information to the SOC while coordinating support to Cal-CSIC and CA-ESF 18. The CA-ESF 18 Coordinator position must be filled by an individual with knowledge of both cyber response and emergency management, to facilitate mutual understanding and cooperation between groups like Cal OES, CDT-SOC, Cal-CSIC, and OIS. The Cal-CSIC Commander or designee will staff this position.

The coordinator also has a role in liaising with other ESF coordinators as necessary for a coordinated response to an event requiring the support of multiple ESFs. In an event where industrial control systems for electrical, water, oil, or gas are implicated/compromised, the CA-ESF 18 Coordinator might serve as the liaison between the response community addressing the public impact of the loss of utilities with the cyber component of the event. The coordinator is responsible for maintaining ESF contact information, gathering and coordinating status reports and other essential elements of information (EEIs) among ESF stakeholders, ensuring consistent messaging and communication protocols across ESF partners, preparation of mission ready packages (MRPs), and documentation. The CA-ESF 18 Coordinator plays a key role in ensuring effective collaboration and communication between CA-ESF 18 and other ESFs, which is essential to well-coordinated incident response. **Table 7** defines the responsibilities of the CA-ESF 18 Coordination Team throughout each of the incident management phases.

Table 7: CA-ESF 18 Coordination Team Responsibilities

Coordination Team Responsibilities
Preparedness and Mitigation
– Maintain the CA-ESF 18 Annex and support an iterative and collaborative planning process
– Build the state's capacity to collectively respond to cyber incidents: – Conduct cybersecurity awareness training and exercises, in coordination with Cal OES to increase awareness about cyber hygiene and best practices – Conduct cybersecurity training and exercises to continuously validate planning concepts and operations
– Establish and maintain working relationships with local, county, state, and federal entities to support the improvement of state response capabilities and improve coordination
– Monitor information and potential threats using multiple information pathways (e.g., Open-Source Intelligence [OSINT], coordination with fusion centers)
– Conduct cyclical analysis of risk to assess and achieve operational benchmarks
– Oversee the implementation of processes to mitigate against the impacts of cyber incidents, including, but not limited to: – Performing recurring data backup – Maintaining off-site data storage – Maintaining awareness of alternate facilities and Point of Contact information – Performing security device configuration reviews – Continuously reviewing state networks and services policies and procedures
– Develop and revise incident handling and reporting plans, protocols, and policies on a continuous basis, and subsequently publicize those changes with relevant audiences
– Identify resources to support incident preparedness, response, and recovery and training stakeholders on available resources
– Maintain and train the IRT
– Maintain and update all local, county, state, federal, and commercial contact lists and test contact methods on at least a quarterly basis
– Maintain relationships and contact information for all other ESFs.

Coordination Team Responsibilities
Response
– Detect and triage potential cyber incidents
– Develop and coordinate threat alerts and critical bulletins
– Analyze the event and articulate potential impacts to relevant stakeholders and state leadership
– Document facts, gather and maintain evidence as needed to support criminal investigations, coordinating with the affected entity for key threat indicators
– Schedule an initial conference with the affected entity to assess the incident, classify its severity on the severity matrix, determine Lead entity within Cal-CSIC and the parties needed to support the IRT, and activate the IRT
– Activate and execute pertinent response plans
– Notify the SOC of any changes to the incident severity level
– Provide regular briefings or updates to elected officials and/or department leadership
– Deploy tactics to contain, eradicate, and recover from a cyber incident
– Ensure confidentiality, integrity, and availability of all information related to the incident
– Report incidents using proper incident handling or notification protocols to all relevant local, county, state, federal, and commercial entities as outlined in the JCIRG
Recovery
– Perform after-action analysis, develop an after-action report, and address corrective action items
– Participate in after action analysis conducted by the state and other ESFs upon request
– Support damage assessments, as needed

Incident Response Team

The IRT will be comprised of agencies from each of the four lines of effort described in **Table 6**. During the initial conference between the affected entity and Cal-CSIC, Cal-CSIC will determine the appropriate membership of the IRT and activate members accordingly. Cal-CSIC will also be responsible for designating the IRT Team Leader.

Upon activation, the IRT will be responsible for:

- Implementing tactical response operations to detect, analyze, contain, eradicate, and recover from an incident within their respective line(s) of effort
- Receiving strategic direction and guidance from Cal-CSIC and aligning response actions appropriately
- Coordinating with public and private sector entities within the state to implement proper threat detection, reporting, and response procedures
- Establishing a regular reporting schedule to provide updates to Cal-CSIC to create and maintain situational awareness and support operational coordination and coordinating with Cal-CSIC to:
    - Conduct briefings or share information with non-state partners
    - Provide recurring reporting to Federal entities using designated reporting procedures to meet regulatory requirements, and create and maintain situational awareness at the federal level
- Providing support to law enforcement agencies responsible for criminal investigation during cyber incidents and state agencies responsible for advancing information security
- Facilitating the collection and proper handling of evidence
- Providing technical support to the affected entity to facilitate cyber incident resolution

Supporting Agencies/Departments

Supporting agencies and departments provide support to primary and lead agencies. **Table 8** Identifies the supporting agencies for CA-ESF 18. Certain supporting agencies are designated by law in California Government Code 8586.5; these agencies are marked with an asterisk.

Table 8: Supporting Agencies/Departments

Supporting Agencies/Departments
Cal OES*
California Business, Consumer Services and Housing Agency (BCSH)
California Community Colleges*
California Department of Corrections and Rehabilitation (CDCR)
California Department of Food and Agriculture
California Department of Veterans' Affairs
California Energy Commission
California Environmental Protection Agency
California Government Operations Agency
California Governor's Office
California Health and Human Services Agency*
California Labor and Workforce Development Agency
California Natural Resources Agency
California Public Utilities Commission (CPUC)
California State Board of Equalization
California State Controller's Office
California State Superintendent of Public Instruction
California State Transportation Agency (CalSTA)
California State Treasurer's Office
California State University*

Supporting Agencies/Departments
California Utilities Emergency Association*
CHP*
CMD*
DHS*
FBI*
Insurance Commissioner of California
Office of the Attorney General*
Office of the Lieutenant Governor of California
OIS*
Other members designated by the Director of Emergency Services*
Secretary of State of California
STAC*
United States Coast Guard*
United States Secret Service*
University of California*

Governor's Task Force on Cybersecurity

California state law stipulates that Cal-CSIC shall develop a statewide cybersecurity strategy, to be informed by recommendations from the Governor's Cybersecurity Task Force. To fulfill these requirements, the Governor's Task Force on Cybersecurity may:

- Inform the state's approach to cybersecurity by providing input during standing meetings or other types of engagement
- Represent the security perspective of assigned state agency during planning, training, exercises, and after-action reporting related to the state cybersecurity strategy
- Attend training, exercises, and planning meetings related to the cybersecurity strategy

Private Sector Stakeholders

Private sector stakeholders in the State of California comprise a diverse group of entities with resources and subject matter expertise related the cyber incident response. These stakeholders also include those who own critical infrastructure and key resources (CIKR). As such, private sector stakeholders may have a significant role with cyber incident management. However, these stakeholders operate outside the public sector and therefore coordinate with state entities in a targeted way.

When a cyber incident impacts a private sector stakeholder, the stakeholder is responsible for providing situational awareness to authorities in accordance with applicable laws, contracts with state government, and industry regulations. It is optional for private sector entities to inform RFCs or Cal-CSIC of cyber incidents. Beyond the established legal requirements, support from the state is provided to private sector entities only as requested. Information applicable to private sector coordination can be found in the engagement materials in **Attachment F**. If the affected entity is not a private sector stakeholder, third-party cybersecurity resources may act as part of the IRT under the Asset Response and Affected Entity Response lines of effort, contributing to response activities through the provision of resources, support, and subject matter expertise on a voluntary basis (see **Figure 1**).

Both private sector partners and governmental partners can benefit from establishing partnerships for response coordination. Although the state and private sector stakeholders do not have the same obligations or responsibilities to one another as governmental entities, each of these groups has specialized skills, equipment, personnel, or expertise which may be advantageous to use cooperatively. To enhance coordination between private sector stakeholders and CA-ESF 18, future actions should be taken to formalize communications and coordination pathways. This may include the development of mission ready packages or mutual aid agreements to facilitate more streamlined coordination during cyber response operations.

Section 3

Concept of Coordination

General

Section 3—Concept of Coordination describes how the CA-ESF 18 will coordinate with and engage supporting partners to conduct operations across mitigation, preparedness, response, and recovery.

Annex Activation

This Annex is always active to support the ongoing detection and analysis of potential cyber incidents. Portions of this Annex may be activated at the discretion of the Cal-CSIC Commander to support cyber incident response. The escalation and de-escalation of cyber incidents will be driven by the thresholds captured in **Table 9**. Escalation and de-escalation may not follow the incremental process depicted in **Table 9** but may skip over levels depending on the severity of the event at the time of discovery or the speed with which the incident is contained. De-escalation of Cal-CSIC's involvement will also be at the discretion of the Cal-CSIC Commander; not the impacted jurisdiction.

Table 9: Escalation and De-Escalation Thresholds

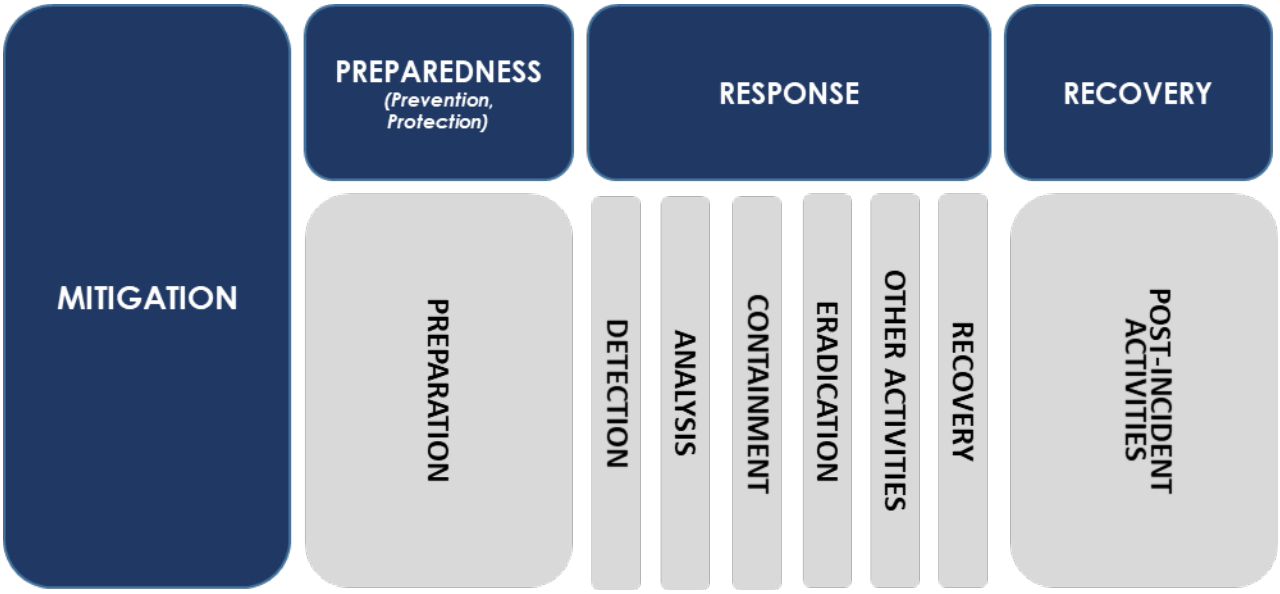
Cyber Incident Severity Level	Escalation Threshold(s)	De-Escalation Threshold(s)
Level 0—Steady State "Steady State" is considered to be an unsubstantiated or inconsequential event.	***Escalate to "Low" if:*** A potential cyber event or incident is suspected, investigated, and classified as an incident that is **unlikely** to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	***Remain at "Steady State" if:*** – The findings of the preliminary investigation reveal that the suspicious activity is not malicious. – The conditions that caused the change have been remediated.
Level 1—Low "Low" severity cyber incidents are unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	***Escalate to "Medium" if:*** A potential cyber event or incident is suspected, investigated, and classified as an incident that **may** impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	***Return to "Steady State" if:*** – The incident is completely resolved, and the agencies confirm that impacted resources and infrastructure are working normally. – The incident is fully contained, and the root cause is identified. – The special event has passed and there is no longer a need to take additional security measures.
Level 2—Medium "Medium" severity cyber incidents may impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	***Escalate to "High" if:*** A potential cyber event or incident is suspected, investigated, and classified as an incident that is **likely to result in a demonstrable impact** to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	***Return to "Low" if:*** – The incident meets the escalation criterion identified within that section.

Cyber Incident Severity Level	Escalation Threshold(s)	De-Escalation Threshold(s)
Level 3—High "High" severity cyber incidents are **likely to result in a demonstrable impact** to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	***Escalate to "Severe" if:*** The cyber incident is **likely to result in a significant impact** to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	***Return to "Medium" if:*** – The incident meets the escalation criterion identified within that section.
Level 4—Severe "Severe" cyber incidents are **likely to result in a significant impact** to public health or safety, national security, economic security, foreign relations, or civil liberties.	***Escalate to "Emergency" if:*** The cyber incident poses an **imminent threat** to the provision of wide-scale critical infrastructure services, State government security, or the lives of California citizens.	***Return to "High" if:*** – The incident meets the escalation criterion identified within that section.
Level 5—Emergency "Emergency" cyber incidents pose an imminent threat to the provision of wide-scale critical infrastructure services, State government security, or the lives of California citizens.		***Return to "Severe" if:*** The incident meets the escalation criterion identified within that section.

Cyber Incident Management Phases

Cyber incidents require the involvement of both information technology experts and emergency management. To provide clarity to all sides of the multi-faceted response partners, the following matrix (**Figure 3**) depicts the overlap between emergency management activities and information technology activities, using terminology familiar to each set of stakeholders.

Figure 3: Cyber Incident Management Process in Relation to Emergency Management Phases



Cyber Incident Response Lines of Effort

As described in **Section 2**, there are four lines of effort in cyber incident response: Threat Response, Asset Response, Intelligence Support, and Affected Entity Response. **Table 6** provides a summary of the entities typically involved in each line of effort. These concurrent lines of effort provide the foundation required to synchronize various response efforts before, during, and after a cyber incident. These lines of effort are defined in Table 10.

Table 10: Lines of Effort, Defined

Line of Effort	Definition
Threat Response	Activities include the appropriate law enforcement investigative activities for: – Collecting evidence and gathering intelligence to provide attribution – Linking related incidents and identifying additional possible affected entities – Identifying threat pursuit and disruption opportunities – Developing and executing courses of action to mitigate the immediate threat and facilitating information sharing and coordination with Asset Response efforts
Asset Response	Activities include furnishing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents by: – Identifying other entities possibly at risk and assessing their risk to the same or similar vulnerabilities – Assessing potential risks to the sector or region, including potential cascading effects, and developing courses of action to mitigate these risks – Facilitating information sharing and operational coordination with Threat Response – Providing guidance on how best to utilize state and local resources and capabilities in a timely, effective manner to speed recovery
Intelligence Support	Facilitates the building of situational threat awareness and sharing of related intelligence to: – Create an integrated analysis of threat trends and events – Identify and assist with the mitigation of knowledge gaps – Suggest methods to degrade or mitigate adversary threat capabilities
Affected Entity Response	– Highly encouraged to share information surrounding the event with other cybersecurity specialists to assist with the investigative, analysis, response, and recovery phases of cyber incident response – The affected entity is the data owner and retains responsibilities to ensure appropriate actions and safeguards are in place to remediate threats and secure their information

Regional Coordination

Successful operation of the state-level CA-ESF 18 requires coordination with a diverse group of stakeholders, including regional partners. RFCs, in particular, play a key role in cyber incident response at the regional level. Fusion centers provide valuable intelligence and response capabilities which can contribute to the mission of CA-ESF 18. This section outlines the role of these fusion centers and identifies methods for coordinating with them.

Coordination Structure

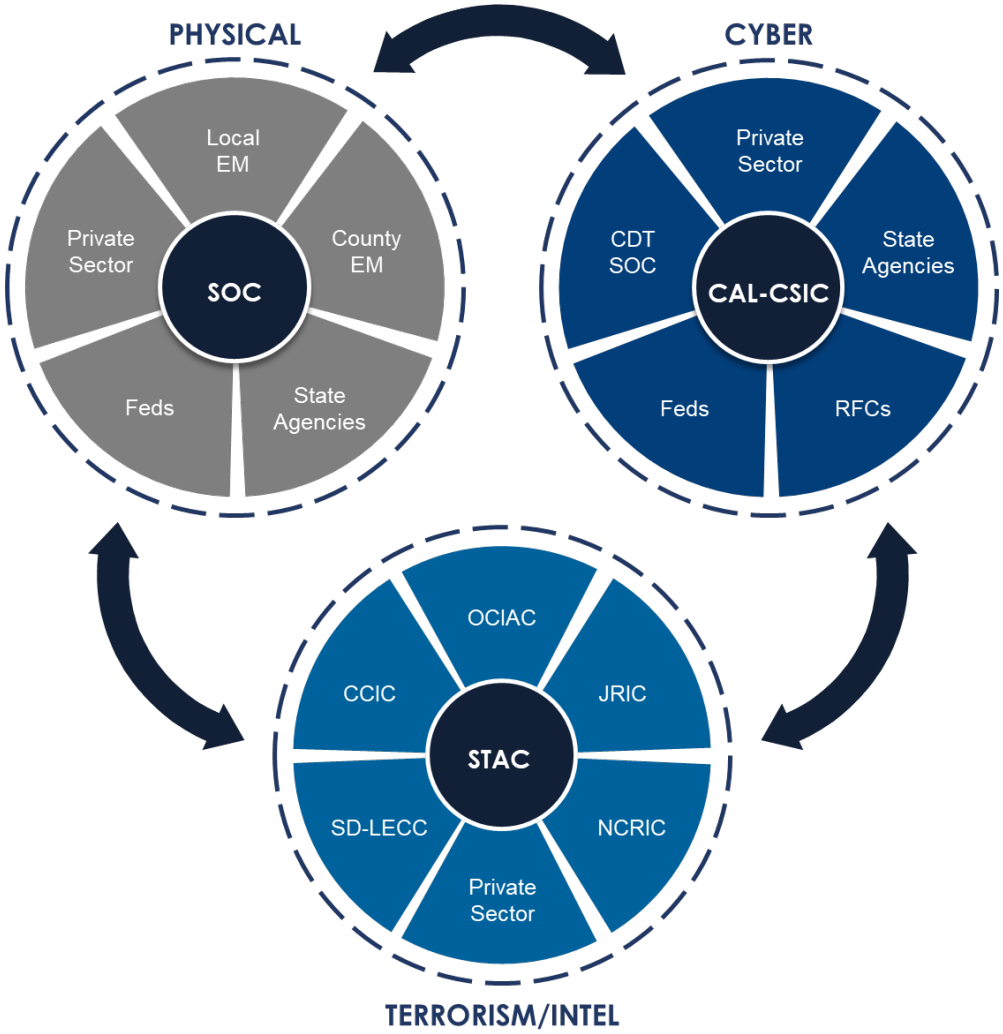
CA-ESF 18 coordinates across a diverse group of stakeholders and entities, with Cal-CSIC serving in a role to facilitate information and resource sharing among ESF partners. Cal-CSIC facilitates cyber coordination among state, local, and federal governmental partners, emergency management, State Threat Assessment Center (STAC), and RFCs. While Cal-CSIC has a formal role in coordinating with federal partners, state and local emergency management, and the STAC, its role in coordination with RFCs is based on requests for support and information sharing.

There are five RFCs in the State of California: the Central California Intelligence Center (CCIC), the Joint Regional Intelligence Center (JRIC), the Northern California Regional Intelligence Center (NCRIC), the Orange County Intelligence Assessment Center (OCIAC), and the San Diego Law Enforcement Coordination Center (SD-LECC). These RFCs request state support for cyber-driven incidents through Cal-CSIC, as stipulated by California state law. Beyond this relationship, RFCs can also look to Cal-CSIC as a resource for information and resources that may be needed to respond to and recover from a cyber incident.

Cal-CSIC's connections with diverse cyber, law enforcement, and emergency management partners allow it to act as a conduit of needed intelligence, equipment, expertise, and staff between partners. In this way, CA-ESF 18 coordinates through Cal-CSIC as the main resource for information and resources during a cyber incident involving response from an CA-ESF 18 partners.

Figure 4 shows the structure of the coordination between CA-ESF 18 stakeholders. This graphic is intended to show the overall structure of coordination and is not inclusive of each of the complex interactions between all ESF partners. Support requests, situational awareness communications, and coordination takes place between many ESF partners. The central entities in each of the functional areas (i.e., SOC, Cal-CSIC, STAC) reflect key coordination points for their functional area, but coordination and communication may take place between any of the entities shown. See **Figure 5** for more specific information on reporting and communications pathways between CA-ESF 18 partners.

Figure 4: CA-ESF 18 Coordination Pathways



Fusion Center Responsibilities

As a key member of CA-ESF 18, a primary responsibility for the RFCs is providing situational awareness on incidents to Cal-CSIC. These fusion centers can provide situational awareness updates to Cal-CSIC even when they are not requesting support from state entities. This one-way communication allows Cal-CSIC to remain aware of ongoing threats and provide expeditious support when requested. Fusion centers may also request state-level incident response support from Cal-CSIC, including support for information and resource sharing. When support is requested, Cal-CSIC can leverage state resources as well as connect regional entities to other actors with a given set of specialized skills or resources. **Table 11** describes the roles and responsibilities of STAC, RFCs, federal partners, and Cal-CSIC for coordinating cyber response. See **Attachment G** for the form that these entities use to inform Cal-CSIC of cyber incidents.

Table 11: Cyber Response Coordination Roles and Responsibilities

STAC	Fusion Centers	Federal Partners	Cal-CSIC
– Collect, analyze, and disseminate intelligence received from RFCs – Act as a clearinghouse for information provided by RFCs – Provide Cal-CSIC with situational awareness updates as necessary – If required, facilitate communications between RFCs and federal partners, ensuring compliance with state and federal laws and safeguarding incident information	– Provide situational awareness on cyber-driven incidents to Cal-CSIC – Provide intelligence support for the incident unless circumstances legally require transitioning ownership (e.g., law enforcement involvement) – Provide status updates to Cal-CSIC as the event progresses – Submit requests for support to Cal-CSIC or federal partners as needed to support response – Participate in regular coordination calls and other communications with Cal-CSIC – Designate a single point of contact for communication related to cybersecurity	– Provide subject matter expertise and response support to Cal-CSIC, STAC, or RFCs, as requested or required by law – Receive and share intelligence from RFCs, Cal-CSIC, and STAC in alignment with established legislation and organizational procedures – Safeguard information related to the incident and ensure compliance with federal law throughout the incident – Provide support for investigation or incident response as requested or required by law – Act as the incident lead in cases where the incident impacts critical infrastructure	– Provide support to reporting fusion centers, when requested to do so – Maintain situational awareness about the incident – Facilitate cyber resource and information sharing between fusion centers, state and Federal agencies. – Facilitate cyber resource and information sharing at the state level, including sharing information to RFCs – Provide state resources and support as appropriate and upon request.

Tertiary Response Support

Cal-CSIC may support response to cyber incidents occurring within non-state entities, if requested and if resources are available to support. The following conditions and actions are associated with assistance to non-state entities.

- Monitor the status of the external, non-state entity's cyber incident throughout the event lifecycle
- Provide Cal OES and state leadership periodic updates on the external, non-State entity's cyber incident and whether any aspects of it are\can\may adversely affect California digital technologies, systems, operations, or services
- Initiate the recommendation for IRT stand up if the external, non-state entity's cyber incident reaches a point where it adversely affects California digital technologies, systems, operations, or services up to Level 2 (Medium) or higher

See **Attachment F** for specific information regarding the role of private sector and non-governmental organizations within CA-ESF 18.

Mitigation Activities

Mitigation activities related to cybersecurity and information technology can be undertaken to reduce the likelihood or impact of a cyber incident. These mitigation activities include conducting policy workshops, technical testing, information sharing, threat assessment, risk analysis and alerting, penetration testing, control assessments, and gap analysis. Cal OES will ensure that emergency functions are integrated in mitigation plans and activities including cyber and will provide information to emergency functions regarding mitigation activities relevant to their core functions.

Preparedness Activities

Emergency preparedness is a continuous cycle of planning, organizing, training, equipping, exercising, evaluating, and taking corrective action across mission areas (i.e., prevention and protection) to ensure effective coordination during cyber incident response. The Lead Agency is responsible for overseeing the implementation of the following preparedness activities:

- Maintaining the CA-ESF 18 Annex and support an iterative and collaborative planning process
- Building the state's capacity to collectively respond to cyber incidents by:
    - Conducting cybersecurity awareness training and exercises, in coordination through Cal-CSIC to increase awareness about cyber hygiene and best practices

    - Conducting cybersecurity training and exercises to continuously validate planning concepts and operations
- Establishing and maintaining working relationships with local, county, state, federal, and commercial entities to support the improvement of state response capabilities and improve coordination
- Monitoring information and potential threats using multiple information pathways (e.g. OSINT, coordination with fusion centers)
- Conducting cyclical analysis of risk to assess and achieve operational benchmarks
- Overseeing the implementation of processes to mitigate against the impacts of cyber incidents, including, but not limited to:
    - Performing recurring data backup
    - Maintaining off-site data storage
    - Maintaining awareness of alternate facilities and information
    - Performing security device configuration reviews
    - Continuously reviewing state networks and services policies and procedures
- Developing and revising incident handling and reporting plans, protocols, and policies on a continuous basis, and subsequently publicizing those changes with relevant audiences
- Identifying resources to support incident preparedness, response, and recovery and training stakeholders on available resources
- Maintaining and updating all local, county, state, federal, and commercial contact lists and test contact methods on at least a quarterly basis
- Maintaining and training the IRT

Prevention Activities

CA-ESF 18 stakeholders will support prevention activities upon request from other ESFs or state agencies.

Protection Activities

CA-ESF 18 stakeholders will support protection activities upon request from other ESFs or state agencies.

Response

The following section will describe key response activities and information necessary to respond to a cyber in the State of California.

Detection

The affected entity is responsible for:

- Detecting signs of an incident or responding to a notification of detection from an external entity
- Performing initial exploration of the incident (i.e., triaging)
- Reporting the incident to all relevant state, federal, and commercial entities as outlined in the JCIRG using incident handling and notification protocols:
    - Cyber incidents affecting California Executive Branch entities must be reported to Cal-CSIC via the California Compliance and Security Incident Reporting System (Cal-CSIRS)
    - Cyber incidents affecting California Judicial or Legislative Branches must be reported to the appropriate authorities and in accordance with applicable laws, contracts with state government, and industry regulations, and may be reported to Cal-CSIC
    - Private sector and non-governmental entities must report Cyber incidents including breaches in accordance with applicable laws, contracts with state government agencies, and industry regulations.
    - When appropriate, Cal-CSIC may report cyber incidents to Federal law enforcement and homeland security agencies when they may:
        - Result in a significant loss of data, system availability, or control of systems;
        - Impact a large number of victims;
        - Indicate unauthorized access to, or malicious software present on, critical information technology systems;
        - Affect critical infrastructure or core government functions; or
        - Impact national security, economic security, or public health and safety[4]
    - Cal-CSIC and all CA-ESF 18 partners will remain conscientious of confidentiality of affected entity information, including considerations for not identifying the name of the affected entity in reporting, as legally required.
- Coordinating with law enforcement entities if the CCIU determines that the incident is criminal in nature
- Managing information sharing with the broader public through affected entity public affairs, or in partnership with the Cal OES Public Information Officer (PIO)

[4] Cyber Incident Reporting: A Unified Message for Reporting to the Federal Government, Department of Homeland Security, 2016.

Analysis

During the Analysis phase of the incident, the affected entity is responsible for coordinating with Cal-CSIC to:

- Understand and articulate the impact to operations, including:
  - Functional impact
  - Information impact
  - Recoverability
- Evaluate the threat based on criteria that could impact response, such as the type of incident and whether it impacts critical infrastructure
- Document facts related to the incident
- Ensure the confidentiality, integrity, and availability of all information related to the incident, including the name of the affected entity and other sensitive incident information
- Classify the severity of the incident using the cyber Incident Severity Matrix (**Table 2**)
- Schedule an initial meeting to assess and determine lead assistance for the incident and determine membership of the IRT
  - Activate the IRT
- Activate and execute pertinent response plans, or overlapping response plans (e.g., continuity of operations, continuity of government)
- Coordinate with law enforcement entities if the CCIU determines that the incident is criminal in nature
  - If the affected entity is a State Executive Branch entity, the state agency will assist law enforcement with evidence collection and root cause determination
- Provide constant monitoring of the threat and situational awareness updates to the IRT and Cal-CSIC

The Cal-CSIC may automatically engage in escalation procedures based on the severity of the incident. When a cyber incident is detected, analyzed, and categorized as (or when it is escalated to) "Severe" or "Emergency" severity, Cal-CSIC will notify Cal OES of the change. This will enable Cal OES to:

- Assess the need for partial or full activation of the SOC
- Activate statewide continuity of operations or continuity of government plans
- Assist with issuing alerts and warnings to the public (if required)

Containment

Cal-CSIC is responsible for coordinating with the affected entity to:

- Notify the SOC of any changes to the severity level
- Provide information to elected officials or department leadership, as requested or otherwise at regular intervals
- Request support from external stakeholders to facilitate containment
- Share information to IRT team members and various intelligence channels

The IRT, Cal-CSIC, and the affected entity will coordinate with partners from relevant lines of effort to:

- Develop and employ sufficient methodologies (via a containment plan) to contain the incident in order to minimize continued impact and/or disruption of services while reducing the likelihood of contamination to other services
- Continue to gather and analyze information about the incident, in order to evolve the remediation strategy as the incident progresses
- If the affected entity is a State Executive Branch entity, they will:
    - Establish a point of contact for media inquiries in case of escalation
    - Keep its Directorate/Cabinet-level informed
- Continue to document facts related to the incident
- Gather and handle evidence, in coordination with relevant external partners, and according to the lines of effort designated Table 6: Lines of Effort and Possible Participating Entities.
- If possible, identify the attacking host or hosts

Eradication

The IRT, Cal-CSIC, and the affected entity will coordinate to:

- Determine how to effectively and safely remove the source of the incident; including measures to scan every device on the affected network segment
- Evaluate the need to change the severity rating of the incident
- Share information to IRT team members and various intelligence channels
- Identify actions to remediate remaining incident impacts

Recovery

The IRT, Cal-CSIC, and the affected entity will coordinate to:

- Determine a phased approach to recovery, if one is not captured or described in other plans, policies, or procedures
- Execute relevant backup strategies to perform data restoration

- Implement corrective actions based on the identified root cause, as applicable
- Perform service recovery
- Perform site recovery

Other Response Activities

Incident Reporting and Notification
The affected entity is responsible for:

- Reporting the incident to authorities in accordance with applicable laws and agreements and activating incident handling protocols, including the following steps (which can occur in the order listed or simultaneously):
    - Report the incident within the organization in accordance with the appropriate, approved IRP
    - Contact the appropriate law enforcement agency (e.g., city, county, state) as applicable
    - Contact the appropriate state-level cybersecurity organization (e.g., Cal-CSIC) as applicable
        - Reporting to Cal-CSIC is optional for all entities except State Executive Branch entities
        - State entities will use Cal-CSIRS to report incidents at the state level
        - Cal-CSIC and all CA-ESF 18 partners will remain conscientious of confidentiality of affected entity information, including considerations for not identifying the name of the affected entity in reporting, as legally required.
    - Adhere to legal notification responsibilities, as described in the JCIRG
    - Notify RFCs of the incident
- Managing information sharing with the broader public through affected entity public affairs, or in partnership with the Cal OES PIO

Demobilization

As resources are no longer needed to support the phase or subtask of a given response activity, or the response activities cease, resources are demobilized. Demobilization includes provisions to address and validate the safe return of resources to their original location and include processes for resource tracking and associated reimbursement. Where applicable, the demobilization should include compliance with mutual aid and assistance provisions. The CA-ESF 18 Coordinator will work with Technical Working Group Chairs to demobilize resources, such as personnel, and ensure that the appropriate documentation is in place to facilitate reimbursement. CDT-SOC, Cal-CSIC, CCIU, and CMF will coordinate to confirm de-escalation of the CA-ESF 18 in accordance with the escalation framework.

Transition to Recovery

CA-ESF 18 may remain active in support of recovery activities aligning with the National Disaster Recovery Framework.[5] Many core functions within the ESFs continue through recovery and require continued coordination with federal ESF counterparts.

Operations will transition from response to recovery when the following conditions are met:

- The Cal-CSIC Commander requests demobilization of Cal-CSIC or the IRT
- The cyber incident severity rating is de-escalated to Steady State
- Cal-CSIC and/or the affected entity initiate recovery of impacted systems and networks
- There are no imminent threats to life safety on the horizon

Post-Incident Activities

Cal-CSIC will coordinate with the IRT and the affected entity to perform after-action analysis, develop an after-action report, and address or implement corrective action items. CA-ESF 18 stakeholders will also participate in after-action analysis conducted by the state and other ESFs upon request.

Depending on the extent of damage to the physical world, damages may be assessed, local jurisdictions may open local assistance centers and emergency recovery centers, and hazard mitigation surveys may be performed.

CA-ESF 18 stakeholders will continue to support network and system assessments, network and system restoration, and other necessary functions to support recovery operations. CA-ESF 18 stakeholders will return to mitigation activities.

[5] Available at: https://www.fema.gov/media-library/assets/documents/117794.

Section 4

Annex Maintenance

Annex Maintenance Overview

The CA-ESF 18 Coordination Team is responsible for the review, updates, and general maintenance of the Annex. Cal-CSIC, will lead annex maintenance efforts and ensure future revisions reflect the inclusion of additional stakeholders, the expansion of resources and capabilities, or the revision of policies and procedures. Revisions shall be approved by Cal OES and members of the supporting state agencies.

Additionally, CA-ESF 18 stakeholders will exercise the concepts outlined in this Annex on an annual basis to support the further development of coordination and collaboration concepts for emergency response in California.

Annex Maintenance Strategies

The Annex maintenance strategies list provides the activities that support the scope of CA-ESF 18. **Table 12** provides a timetable and checklist for stakeholders of CA-ESF 18 to address these critical goals and to ensure that existing protocols are current and efficient. Annual updates are recommended for this Annex.

Table 12: CA-ESF 18 Maintenance Strategy Tasks

Critical Maintenance Activity	Task	Task Lead	Frequency
1. Review roles and responsibilities.	Identify the roles and responsibilities of the CA-ESF 18 Coordinator, the CA-ESF 18 Coordination Team, and Cal-CSIC strategic partners within the Annex.	CA-ESF 18 Coordinator	Every 3 Years, or as needed
2. Maintain partnerships within the structure of the CA-ESF 18.	Identify and integrate partners from the private sector, NGOs, other ESFs, and the emergency management community.	Cal-CSIC	Every 3 Years
3. Update stakeholder contact information.	Identify the lead point of contact for each CA-ESF 18 stakeholder agency, including phone, email, and after-hours contact information, as well as the contact information for the agency/department emergency operations center.	CA-ESF 18 Coordinator	Annually

Critical Maintenance Activity	Task	Task Lead	Frequency
4. Revise the CA-ESF 18 Annex.	Review and update as needed all sections of the CA-ESF 18 Annex.	CA-ESF 18 Coordinator	Every 3 Years

Annex Updates

The CA-ESF 18 Annex will be updated as needed. Thresholds for reviewing and updating this Annex include, but are not limited to:

- Changes to state or federal law or emergency management procedures;
- Critical corrective actions to address lessons learned from activations and/or exercises;
- Development of or advancement in emergency response capabilities;
- Periodic review as recommended by SEMS; and
- Changes to personnel contact information.

Proposed changes should complement existing authorities, regulations, statutes, and other plans (see **Table 5** for the linkage to other plans). After the updates to the Annex have been made, a summary of the changes should be sent out to all CA-ESF 18 stakeholders with the updated document. **Table 13** should be updated to reflect all revisions to the Annex.

Table 13: Annex Revisions

Version	Date	Summary of Changes
Inaugural Edition	January 2020	Original publication

Attachment A

Acronyms and Definitions

Acronyms

Table 14: Annex Acronyms

Acronym	Meaning
BCSH	California Business, Consumer Services and Housing Agency
CA-DOJ	California Department of Justice
Cal OES	California Office of Emergency Services
Cal-CSIC	California Cybersecurity Integration Center
Cal-CSIRS	California Compliance and Security Incident Reporting System
CalSTA	California State Transportation Agency
CDCR	California Department of Corrections and Rehabilitation
CDT	California Department of Technology
CDT-SOC	California Department of Technology Security Operations Center
CHP	California Highway Patrol
CHP-CCIU	California Highway Patrol- Computer Crimes Investigation Unit
CCIC	Central California Intelligence Center
CICE	California Joint Cyber Incident Communications and Escalation Framework
CIKR	Critical Infrastructure and Key Resources
CISO	Chief Information Security Officer
CMD	California Military Department
CMF	Cyber Mission Force
CPUC	California Public Utilities Commission
DHS	Department of Homeland Security
DHS NCCIC	Department of Homeland Security National Cybersecurity and Communications Integration Center
EEI	Essential Elements of Information

Acronym	Meaning
EMAC	Emergency Management Assistance Compact
ESF	Emergency Support Function
FBI	Federal Bureau of Investigation
FMA	Flood Mitigation Assistance
GIS	Geographic Information Systems
GPS	Global Positioning System
HMGP	Hazard Mitigation Grant Program
IRP	Incident Response Plan
IRT	Incident Response Team
ISO	Information Security Officer
IT	Information Technology
JCIRG	Joint Cyber Incident Response Guide
JFO	Joint Field Office
JRIC	Joint Regional Intelligence Center
MRP	Mission Ready Package
MS-ISAC	Multi-State Information Sharing and Analysis Center
NASCIO	National Association of State Chief Information Officers
NCCIC	National Cybersecurity and Communications Integration Center
NCCFRP	Northern California Catastrophic Flood Response Plan
NCIRP	National Cyber Incident Response Plan
NCRIC	Northern California Regional Intelligence Center
NGO	Non-Governmental Organization
NIMS	National Incident Management System
NIST	National Institute of Standards and Technology
OCIAC	Orange County Intelligence Assessment Center
OIS	Office of Information Security
OSINT	Open-Source Intelligence
PDM	Pre-Disaster Mitigation
PIO	Public Information Officer
PPD	Presidential Policy Directive

Acronym	Meaning
REOC	Regional Emergency Operations Center
RFC	Regional Fusion Center
SD-LECC	San Diego Law Enforcement Coordination Center
SEMS	State Emergency Management System
SEP	State Emergency Plan
SHMP	State Hazard Mitigation Plan
SLTT	State, Local, Tribal, and Territorial
SOC	State Operations Center
SRL	Severe Repetitive Loss
STAC	State Threat Assessment Center
STAS	State Threat Assessment System
WebEOC	Web Emergency Operations Center

Attachment B

Cal SOC and Cal-CSIC Interaction

During incidents that are either cyber-driven or have cyber impacts, decisions and activities require coordination between Cal-CSIC and the SOC in order to respond effectively.

Table 15 below compares the California SOC activation levels with the Cal-CSIC severity levels. This comparison is presented to show how the severity and activation levels between the SOC and Cal-CSIC will interact during an incident. During events that are cyber-driven but have wider impacts (e.g., physical impacts), the Cal-CSIC severity levels will be used to describe the severity of the cyber incident, while the SOC activation levels will be used to describe the level of operations the SOC is taking in response to the incident.

The use of the activation and severity levels is also consistent with how such events are managed. During incident response, the SOC maintains control over consequence management, while Cal-CSIC leads the cyber operations within the incident. These cyber operations include supporting fusion centers as requested, facilitating resource and information sharing among fusion centers and between fusion centers and federal partners, and providing resources and support through private sector partners.

Table 15: SOC and Cal-CSIC Activation Level Interaction

California State Operations Center		California Cybersecurity Integration Center		
Description	**Activation Level**	**Cyber Incident Severity**	**Description**	**Level of Effort—Description of Actions**
N/A	**N/A**	**Level 0—Steady State**	Unsubstantiated or inconsequential event.	Steady State, which includes routine watch and warning activities.
Level Three is a minimum activation. This level may be used for situations which initially only require a few people, e.g., a short-term earthquake prediction at level one or two; alerts of storms, or tsunamis; or monitoring of a low-risk planned event. At a minimum, Level Three staffing consists of the EOC Director, Section Coordinators, and a situation assessment activity in the Planning and Intelligence Section. Other members of the organization could also be part of this level of activation e.g., the Communications Unit from the Logistics Section, or an Information Officer.	**Level 3**	**Level 1—Low**	Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	Requires coordination among State Departments 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 2—Medium	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.

California State Operations Center		California Cybersecurity Integration Center		
Description	**Activation Level**	**Cyber Incident Severity**	**Description**	**Level of Effort—Description of Actions**
Level Two activation is normally achieved as an increase from Level Three or a decrease from Level One. This activation level is used for emergencies or planned events that would require more than a minimum staff but would not call for a full activation of all organization elements, or less than full staffing. The EOC Director, in conjunction with the General Staff, will determine the required level of continued activation under Level Two, and demobilize functions or add additional staff to functions as necessary based upon event considerations. Representatives to the EOC from other agencies or jurisdictions may be required under Level Two to support functional area activations.	**Level 2**	**Level 3—High**	Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	Requires elevated coordination among State Departments, State Agencies, or SLTT governments due to moderate levels and breadth of damage. Potential involvement of FEMA and other federal agencies.
		Level 4—Severe	Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.	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.

California State Operations Center		California Cybersecurity Integration Center		
Description	**Activation Level**	**Cyber Incident Severity**	**Description**	**Level of Effort—Description of Actions**
Level One activation involves a complete and full activation of all organizational elements at full staffing and all Emergency Support Functions. Level One would normally be the initial activation during any major emergency requiring extreme State level help.	**Level 1**	**Level 5—Emergency**	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, size, location, 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.

Attachment C

Communications Guidance

Introduction

This attachment outlines the communication pathways, methods, and policies to be implemented within CA-ESF 18 to ensure effective information sharing, coordination, situational awareness updates, and mutual understanding of response goals and activities. Communications and information sharing are significant components in cyber response, which requires active coordination between diverse stakeholders. This guide includes information on how the information sharing process will be carried out between CA-ESF 18 partners and identifies the primary, secondary, and tertiary communications pathways that exist to ensure the availability of communications methods during a cyber incident which may compromise telecommunications methods.

Purpose

This attachment acts as a supplement to the Concept of Coordination in the base plan, providing a specific tactical approach to communications during activation of CA-ESF 18. Using the coordination structure and relationships establishing in the plan and in other existing plans, policies, and laws, this attachment provides an overview of how CA-ESF 18 will coordinate and the methods CA-ESF 18 will use to share information.

Scope

Communications guidance contained in this attachment is intended to be used in alignment with all existing laws, plans, and policies. Existing privacy laws and policies and other legal requirements are to be upheld during the use of the following information sharing processes and communications pathways. The following communications guidance is built in accordance with CICE and JCIRG communications stipulations and is not intended to supersede these existing plans. This attachment is intended to be used as a quick reference guide to communications as a companion to the base CA-ESF 18 Cybersecurity Annex and other plans and policies listed in Authorities and References.

Information Sharing Process

Figure 5 represents the desired communications flow between CA-ESF 18 Coordination Team entities. The process is intended to incorporate all stages of information sharing within a cyber incident, including how information is processed, analyzed, and disseminated before, during, and after an incident. **Figure 5** shows the initial flow of notifications from CA-ESF 18 stakeholders, rather than the flow of situational awareness updates during ongoing response operations. At times, stakeholders are requested to

simultaneously notify Cal-CSIC strategic partners to ensure that all parties have the relevant information to successfully execute a coordinated response.

Figure 5: Information Sharing Process

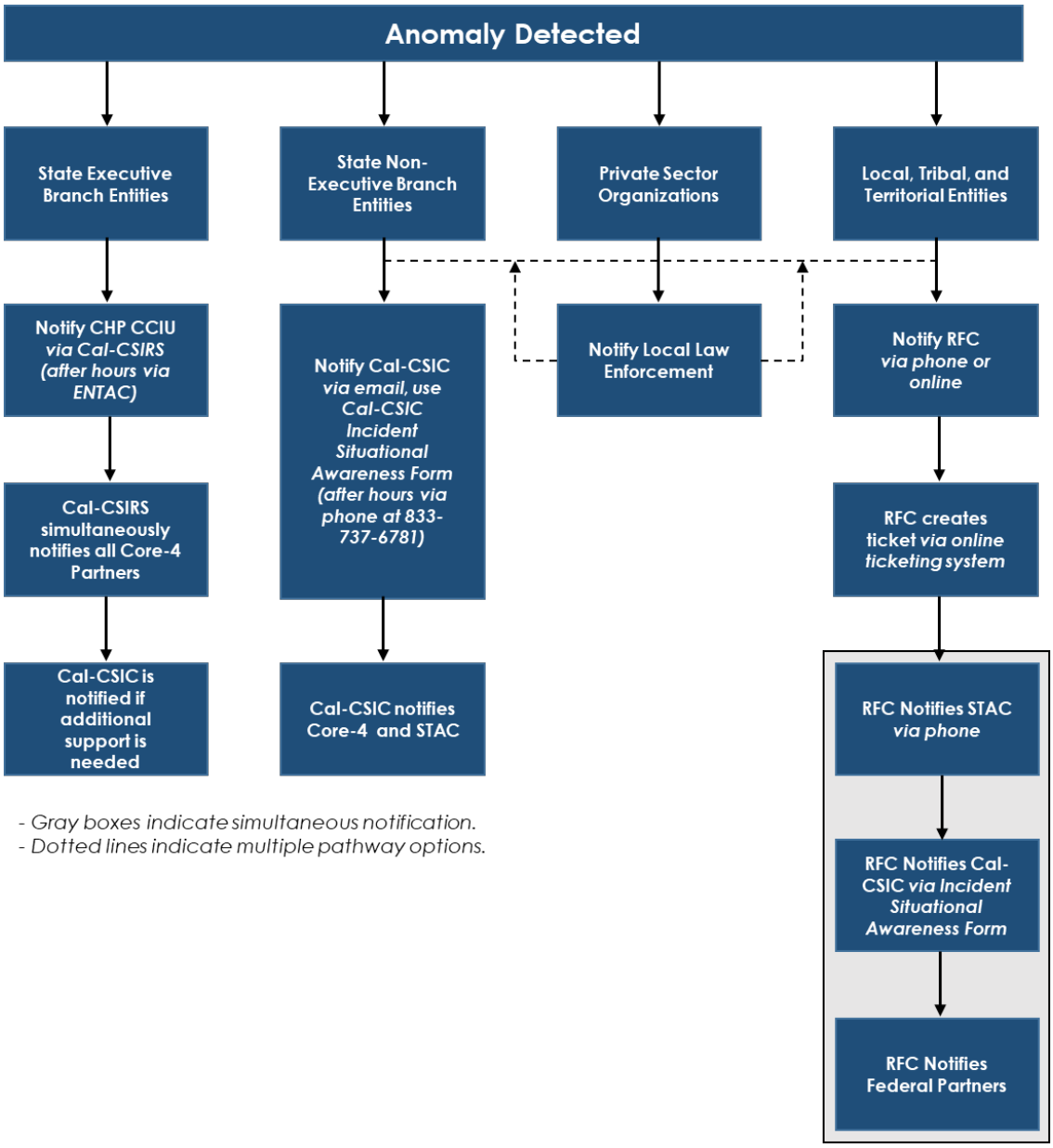


Table 16 identifies the communications tools and resources that exist and can be leveraged to support cyber incident notifications during the activation of CA-ESF 18.

Table 16: Communications Resources

Resource Description	*Primary User(s)*	*Reference(s)/Instructions*
Cal-CSIC. Primary cyber response coordination entity in the State of California. Provides response support.	– State Non-Executive Branch Entities – Private Sector Organizations – Local, Tribal, and Territorial Entities	– Complete the Incident Response Questionnaire – Available by phone at: 1-833-REPORT1 – Available by email at: calcsic@caloes.ca.gov
Cal-CSIC Duty Officer. On-call personnel responsible for mobilizing Cal-CSIC resources after-hours.	– State Non-Executive Branch Entities – Private Sector Organizations – Local, Tribal, and Territorial Entities	Available by phone at: (916) 845-8911
Cal-CSIRS. Online reporting system for state agencies which automatically provides simultaneous notifications to the Cal-CSIC partners. Reports from Cal-CSIRS are sent to CDT-SOC and CHP for analysis support, and Cal-CSIC is notified if additional support is needed.	– State Executive Branch Entities – CDT OIS	– With Cal-CSIRS account: navigate to the database at https://CalCSIRS.rsam.com – Without Cal-CSIRS account: contact the Chief Information Security Officer (CISO) at (916) 445-5239 or by email at security@state.ca.gov
CHP CCIU. California Highway Patrol's Computer Crimes Investigation Unit has primary investigative authority for violations of California Penal Code Section 502, where a state agency is the victim.	– All CA-ESF 18 Members	– Available by phone at: (916) 450-2200
Emergency Notification and Tactical Alert Center (ENTAC). An alert center that is staffed 24/7 and is able to forward notices and alerts to CHP.	– State Executive Branch Entities	– Available by phone at: (916) 843-4199
Incident Situational Awareness Form. Standard reporting form attached to CA-ESF 18 Annex intended to standardize information sharing between fusion centers and Cal OES during ongoing incidents.	– RFCs – STAC	– CA-ESF 18 Annex, Attachment G
STAC. California's state primary fusion center and information sharing clearinghouse.	– All CA-ESF 18 Members	– Available by phone at: (916) 636-2900

Authorities and References

The following plans are relevant to the notification and communications procedures contained in this attachment.

Table 17: Communications Procedures Authorities and References

Authorities and References	
State	
California Government Code Section 8586.5 (2018)	Assembly Bill 2813 added section 8586.5 to the California Government Code, which codified Cal-CSIC in state law. Cal-CSIC was originally the result of Executive Order B-34-15. This government code re-establishes this order as part of California state law.
California Government Code Section 8558 (2018)	Senate Bill 532 amended Section 8558 of the Government Code to include cyberterrorism in the conditions that constitute a state of emergency and local emergency.
Joint Cyber Incident Response Guide (2018)	The Joint Cyber Incident Response Guide (JCIRG) provides guidance for governmental and non-governmental entities within California developing incident response plans (IRPs). CA-ESF 18 works with existing local and regional IRPs that are based on the guidance provided in this document. JCIRG includes information on legal reporting requirements at the state and federal levels. As an incident escalates, these reporting requirements should be followed and met to ensure legal compliance.
Joint Cyber Incident Communications and Escalation Framework (2018)	The Joint Cyber Incident Communications and Escalation Framework facilitates effective communication and ensures incident information is shared with the appropriate entities in a timely manner to enhance the protective posture during all phases of incident response. The framework 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.
State of California Emergency Plan (2017)	The State of California Emergency Plan (SEP) is the base plan to which this document is an annex. The SEP provides general guidance related to incident management and cyber threats. The SEP includes guidance related to communications and information sharing applicable to all ESFs.
State of California Hazard Mitigation Plan (2018)	The State of California Hazard Mitigation Plan (SHMP) includes a hazard profile on cyber threats, which describes in detail the threats California faces from cyber incidents, existing mitigation measures against losses from cyber incidents, and potential new mitigation projects to defend against cyber incidents. The SHMP describes the potential and historical impacts of a cyber incident, and highlights Cal-CSIC's role in encouraging private-public partnerships.

Attachment D
Execution Checklists

The following execution checklists provide procedures for each phase of the incident management process. These checklists are intended to provide a quick reference for the expected roles of key leadership during a cyber incident, and include information on procedures for alert notification, escalation, reporting, public notification, and federal cyber incident reporting, as well as other essential elements of cyber incident management.

These checklists are intended for use by the CA-ESF 18 Lead Agency and ESF Coordinator. These stakeholders should review this CA-ESF 18 Annex and the execution checklists to learn more about their roles and responsibilities before a cyber incident takes place. The Lead Agency and ESF Coordinator may also use these checklists as a reference during a cyber incident.

Table 18: Lead Agency Execution Checklist

Phase	Action	
Mitigation	Performing recurring data backup	☐
	Maintaining off-site data storage	☐
	Maintaining awareness of alternate facilities and information	☐
	Performing security device configuration reviews	☐
Preparedness	Building the state's capacity to collectively respond to cyber incidents: – Conducting cybersecurity awareness training and exercises, in coordination with Cal OES to increase awareness about cyber hygiene and best practices – Conducting cybersecurity training and exercises to continuously validate planning concepts and operations	☐
	Developing and revising incident handling and reporting plans, protocols, and policies on a continuous basis, and subsequently publicizing those changes with relevant audiences	☐
	Identifying resources to support incident preparedness, response, and recovery and training stakeholders on available resources	☐
	Maintaining and training the IRT	☐
Response	Attend an initial meeting to assess and determine lead assistance for the incident and determine membership of the IRT	☐
	Develop and employ sufficient methodologies (via a containment plan) to contain the incident in order to minimize continued impact and/or disruption of services while reducing the likelihood of contamination to other services	☐
	Continue to gather and analyze information about the incident, in order to evolve the remediation strategy as the incident progresses	☐
	Continue to document facts related to the incident	☐
	Gather and handle evidence, in coordination with relevant external partners, and according to the lines of effort designated in Error! Reference source not found.	☐
	If possible, identify the attacking host or hosts	☐
	Determine how to effectively and safely remove the source of the incident; including measures to scan every device on the affected network segment	☐
	Evaluate the need to change the severity rating of the incident	☐
	Share information to IRT team members and various intelligence channels	☐
	Identify actions to remediate remaining incident impacts	☐
Recovery	Execute relevant backup strategies to perform data restoration	☐
	Implement corrective actions based on the identified root cause, as applicable	☐
	Perform service recovery	☐
	Perform site recovery	☐

The following checklist describes the activities that the CA-ESF 18 Coordinator is responsible for.

Table 19: CA-ESF 18 Coordinator Execution Checklist

Phase	Action	
Mitigation	Implement lessons learned from previous trainings, exercises, and cyber incidents to identify vulnerabilities and mitigation efforts to address them	☐
	Identify mitigation activities within the coordination of the ESF that can be carried out to reduce risks related to CA-ESF 18 response efforts	☐
	Identify potential funding sources to support identified mitigation actions	☐
Preparedness	Maintain partnerships with members of Cal OES, CDT-SOC, Cal-CSIC, and OIS in order to build mutual understanding of objectives and functions between response partners	☐
	Maintain all relevant CA-ESF 18 contact information	☐
	Prepare mission ready packages	☐
Response	Facilitate information sharing and coordination between the broader response community and CA-ESF 18 stakeholders	☐
	Facilitate coordination, cooperation, and unity of operations among CA-ESF 18 stakeholders	☐
	Provide information to the SOC and coordinate support to the Office of Information Security (OIS)	☐
	Liaise with other ESF coordinators as necessary for coordinated response	☐
	Gather and coordinate status reports and other essential elements of information among ESF stakeholders	☐
	Request support from other ESFs in their role as outlined in **Table 3**	☐
	Ensure consistent messaging and communication protocols across ESF partners	☐
	Observe and record key lessons learned during incident response to inform after action reporting	☐
Recovery	Prepare after action reporting based on lessons learned and incident documentation	☐
	Facilitate de-activation of the CA-ESF 18 Annex and demobilization of all CA-ESF 18 stakeholders	☐
	Share lessons learned with other ESF coordinators and the broader emergency response community	☐
	Identify actions to implement lessons learned as identified in after-action reporting	☐

Attachment E

Private Sector, NGO, and Tribal Engagement Guide

Introduction

This attachment provides materials and guidance related to engaging private sector entities, non-governmental organizations (NGOs), and tribal entities during cyber incidents. This attachment includes tear-away engagement materials which can be used or modified both during steady state and preparedness operations, or in the event of a cyber incident to engage these partners. The provided materials explain the existing regional and state resources for cyber incident support, as well as delineate the roles and responsibilities of private sector, NGO, and tribal entities within cyber response.

Purpose

This attachment is intended to provide guidance for coordination with private sector, non-governmental, and tribal partners, targeted engagement materials, and a definition of roles and responsibilities for these types of stakeholders. The materials provided in this attachment will act as a roadmap for how to engage with these entities, including tools and language specific to these groups and their role as partners during cyber incidents. Given that cyber incidents can impact any entity, cyber preparedness and building relationships and awareness with partners from all sectors is important. Private sector, NGO, and tribal partners can be an essential source of resources, skills, and support for cyber incident response if properly leveraged. This attachment targets methods for ensuring that non-state entities are sufficiently engaged during cyber operations.

Scope

This attachment provides engagement materials which can be used and adapted for engaging private sector, non-governmental, and tribal entities during steady state and CA-ESF 18 activation. These tools and guidance are intended to be used by CA-ESF 18 stakeholders within their established role and have not been designed to fit the engagement needs of any entity or activation level. Engagement tools can be adapted for use by other entities as appropriate and as permitted by ESF leadership.

Engagement Materials

See the following pages for the private sector, NGO, and tribal engagement materials.

Private Sector, NGO, and Tribal Entities in a Cyber Secure California

The State of California faces a variety of cyber threats which may impact critical infrastructure, public safety, and public perception. To effectively respond to these cyber threats and cyber incidents, diverse stakeholders across the public and private sectors must collaborate and coordinate. Private sector stakeholders, tribal entities, and non-governmental organizations (NGOs) have an essential role in safeguarding California's cyber resources. In 2019, the California Governor's Office of Emergency Services (Cal OES) and the California Cybersecurity Integration Center (Cal-CSIC) worked with a broad stakeholder group to develop an Emergency Support Function (ESF) 18 Cybersecurity Annex to the State Emergency Plan. This Annex describes how entities within the State of California will work together to respond to cyber incidents and includes information for the private sector, tribal entities, and NGOs.

What is Cal-CSIC?

Cal-CSIC was established by Executive Order B-34-15 on August 31, 2015. Cal-CSIC is the central body for state-level cyber incident preparedness, response, and recovery. In its capacity as the Lead entity for CA-ESF 18, Cal-CSIC carries out the following responsibilities dictated by state legislation:

1. Reduce the likelihood and severity of cyber-attacks;
2. Improve inter-agency and cross-sector information coordination;
3. Prioritize cyber threats and alert potential victim entities; and
4. Strengthen the state's cybersecurity strategy

In accordance with its established responsibilities, Cal-CSIC coordinates state-level cyber response efforts. Cal-CSIC serves as the central point of coordination during cyber incidents and facilitates information and resource sharing across stakeholder groups. Cal-CSIC gathers and analyzes situational awareness information from stakeholders such as regional fusion centers and facilitates resource sharing among stakeholders as needed to support cyber incident response. Cal-CSIC also provides strategic intelligence analysis to statewide leadership, policy makers, and non-state partners related to cybersecurity.

What is STAC?

The State Threat Assessment Center (STAC) is a statewide fusion center for the State of California which gathers, analyzes, and disseminates information about threats to

the state. In coordination with regional fusion centers, STAC receives reporting related to suspicious activity, collects and analyzes intelligence, and acts as the clearinghouse for information received from fusion centers. STAC also has a role in coordinating with Cal-CSIC and federal partners. These roles are applicable to cyber threats that may activate CA-ESF 18. The private sector, NGOs, and tribal entities may report to or liaise with STAC during cyber incidents, depending on the severity of the incident.

What is my role in cyber response?

The following roles and responsibilities are captured in the current version of the CA-ESF 18 Annex:

Planning	**Ongoing**	**Response**
Participate in the development of the state's technical response strategy and provide subject matter expertise.	Report suspicious cyber events or incidents in accordance with legal requirements. Facilitate communication with the state.	Provide intelligence or technical assistance (to the extent possible) that may indicate the development of a regional-level disruption event.

How can I engage with CA-ESF 18?

The private sector, NGOs, and tribal entities comprise a network of rich cyber resources, skills, and experience. By coordinating with Cal-CSIC, STAC, or regional fusion centers, these entities can both leverage the state's own network of resources and offer assistance to support affected entities and assets during cyber incident response. Private sector entities, NGOs, and tribal entities can build partnerships with Cal-CSIC and other public sector stakeholders in the following ways:

- Providing subject matter expertise to inform planning and other preparedness efforts;
- Voluntarily reporting cyber incidents to Cal-CSIC, STAC, or regional fusion centers;
- Supporting Affected Entity Response and Asset Response during cyber incidents

How can I report cyber incidents?

Suspicious cyber activity may be detected by any entity, including the private sector, NGOs, or tribal entities. All entities report cyber incidents in accordance with the legal requirements that apply to them. Where not required by federal or state laws, entities may also choose to voluntarily report to STAC, Cal-CSIC, or regional fusion centers.

Your organization may report to Cal-CSIC, STAC, or your regional fusion center using the following methods if an incident is classified as a Level 2 or higher on the severity matrix:

REPORTING METHODS		
STAC	**Cal-CSIC**	**Regional Fusion Centers**
Phone: (916) 636-2900 **Email:** STAC@caloes.ca.gov	**Phone:** (833) REPORT1 or (833) 737-6781	**Find Your Fusion Center:** https://calstas.org

Attachment F

Incident Situational Awareness Form

Introduction

This attachment provides a tear-away reporting form for use by entities within California to encourage communication and reporting to Cal-CSIC in order to support situational awareness and incident response operations during cyber incidents.

Purpose

The Incident Situational Awareness Form is intended to support information sharing and situational awareness about cyber incidents to Cal-CSIC. This form may be completed by any entity providing situational awareness about a cyber incident, including fusion centers and affected entities. This form should be completed and returned to Cal-CSIC when an incident is determined to be a Level 2 or higher on the severity matrix (see **Table 2**). Cal-CSIC does not need to be informed of all cyber incidents. Fusion centers may inform Cal-CSIC of incidents that do not reach this level as aggregate data (i.e., statistics on the total number of incidents by incident type) on a monthly basis.

Scope

The Incident Situational Awareness Form is intended for use by:

- California State Threat Assessment Center (STAC)
- Central California Intelligence Center (CCIC)
- Joint Regional Intelligence Center (JRIC)
- Northern California Regional Intelligence Center (NCRIC)
- Orange County Intelligence Assessment Center (OCIAC)
- San Diego Law Enforcement Coordination Center (SD-LECC)
- Affected entities
- Other reporting entities within the State of California

Incident Situational Awareness Form

The Incident Situational Awareness Form is provided on the following page.

Cal-CSIC Assistance **IS REQUESTED:** ☐

Cal-CSIC Assistance **IS NOT REQUESTED:** ☐

Complete the form and send it via email to Cal-CSIC (calcsic@caloes.ca.gov) and STAC (STAC@caloes.ca.gov) if the incident is determined to be a Level 2 or higher on the severity matrix.

Date and Time:			**Report Version:**	
Name of Person Reporting: ***OPTIONAL***			**Position of Person Reporting:** ***OPTIONAL***	
Reporting Entity:	☐	Joint Regional Intelligence Center (JRIC)	☐	State Executive Branch Entity
	☐	State Terrorism Assessment Center (STAC)	☐	Local, Tribal, or Territorial Entity
	☐	Central California Intelligence Center (CCIC)	☐	State Non-Executive Branch Entity
	☐	San Diego Law Enforcement Coordination Center (SD-LECC)	☐	Private Sector Organization
	☐	Northern California Regional Intelligence Center (NCRIC)	☐	Other (Please describe):
	☐	Orange County Intelligence Assessment Center (OCIAC)		
Are You the Affected Entity?	☐	Yes *(If yes, please skip to "Affected Entity Name.")*	☐	No *(If no, please select the affected entity type below.)*
Affected Entity Type:	☐	State Executive Branch Entity	☐	State Non-Executive Branch Entity
	☐	Local, Tribal, or Territorial Entity	☐	Private Sector Organizations
	☐	Regional Fusion Center	☐	Other (please describe):
Affected Entity Name: ***OPTIONAL***[6]				

[6] REMINDER: All ESF 18 partners will remain conscientious of confidentiality of affected entity information, including considerations for not identifying the name of the affected entity in reporting, as legally required.

Date and Time:		**Report Version:**	
Contact Information of Affected Entity: ***OPTIONAL***			
Date/Time of Incident:		**Date/Time Discovered:**	
Critical Infrastructure and Key Resources Potentially Affected:	☐ Chemical ☐ Commercial Facilities ☐ Communications ☐ Critical Manufacturing ☐ Dams ☐ Defense Industrial ☐ Emergency Services ☐ Energy	☐ Financial Services ☐ Food and Agriculture ☐ Government Facilities ☐ Healthcare and Public Health ☐ Information Technology ☐ Nuclear Reactors/Material/Waste ☐ Transportation Systems ☐ Water and Wastewater	
What is the Incident Severity Level? *[Provide current Severity level and impact]*			
What is the Root Cause of the Incident? *[e.g., carelessness, inadvertent, intentional, loss, theft, damage]*			
Description of Incident:			
Actions Taken Prior to Reporting:			
Is the Incident Contained?			

Attachment G

Bi-Weekly Synchronization Call Agenda

The agenda found in **Table 20** is intended to be used bi-weekly, or at an appropriate interval as determined by CA-ESF 18 partners, to ensure that members of CA-ESF 18 have an opportunity to meet and discuss pertinent issues which may arise during steady state operations or during CA-ESF 18 activation. The bi-weekly synchronization call establishes a two-way communication pathway between CA-ESF 18 partners by allowing stakeholders from state agencies, regional fusion centers, local governments, and private sector businesses to share information and address issues relevant to the ESF during steady state or activation. These calls will be centered on providing situational awareness and updates on significant events that may impact the ESF and its potential for activation, or on the progress of incident response activities. This agenda may also support existing standing calls between CA-ESF 18 stakeholders and does not necessarily stipulate the creation of a new call between stakeholders if a suitable two-way communication pathway already exists.

Table 20: Coordination Call Agenda

Conference Details			
Date:		**Time:**	
Conference Line/Access Code:			
Call/Meeting Host:			
General Guidelines			
Conference Call Etiquette	– Do not place the phone "on hold" as it puts everyone on the call on hold. – Mute your phone to lessen background noise. – Be respectful of the person speaking and minimize side conversations or interruptions. – The host will provide participants with an opportunity to ask questions.		
Attendance/Roll Call			
Attendance	Name _____ Agency: _____ Name _____ Agency: _____ Name _____ Agency: _____ Name _____ Agency: _____ Name _____ Agency: _____ Name _____ Agency: _____ Name _____ Agency: _____		
Overview/Purpose			
Agenda Item	**Notes**		
Call/Meeting Purpose			

CA-ESF 18 Update	
Agenda Item	**Notes**
What is the Incident Severity Level? *[Provide current severity level. Identify any potential for escalation or activation.]*	
Ongoing Issues and Concerns *[Provide updates on ongoing concerns related to the function of the ESF and how these issues are being addressed. Identify any needed support.]*	
Regional Fusion Center Sync-up *[Fusion centers will provide any necessary situational awareness updates and identify any support needs related to information or resource sharing.]*	
Review Action Items	
Other Updates	

Summary	
Action Item	**Responsible Party**

Next Conference Call/Meeting			
Date:		**Time:**	
Conference Line/Access Code:			

Attachment H

Resource Sharing Guidance

Introduction

This attachment describes how stakeholders will coordinate to share resources during cyber incident response. Resources include equipment and personnel that may be employed to respond to a cyber incident. This section outlines significant resource sharing pathways, including mutual aid, mission ready packages, and federal support. The information in this section is intended to be used as a reference for establishing resource sharing partnerships and for seeking resource support during a cyber incident.

Purpose

The resource sharing guidance is intended to help build awareness of resource sharing pathways and provide information on how to build partnerships for resource sharing. The ability to efficiently share resources between stakeholders is a key capability for ensuring that affected entities and their mission partners are adequately equipped to respond to cyber incidents. Members of CA-ESF 18 may use the resource sharing information in this attachment to guide interactions with other CA-ESF 18 members, or with other mission partners from the private and public sectors. This attachment identifies existing pathways for resource sharing and provides guidance for using these pathways during response.

Scope

The resource sharing guidance contained in this attachment is to be used as a supplement to existing policies, plans, and laws that dictate how entities request and provide shared resources during cyber incident response. This guidance is not intended to supersede existing agreements or divert existing reporting pathways. This attachment serves as a quick reference for resource sharing sources and procedures.

Resource Sharing Guidance

Mutual Aid

The following section outlines current mutual aid systems and processes, at national, state, and local levels. The National Incident Management System (NIMS) is a comprehensive, national approach to incident management which can be applied at all levels of government. As a component of NIMS, mutual aid agreements are discussed in detail in the NIMS Guideline for Mutual Aid. This document addresses the different types of mutual aid agreements, the key elements of a mutual aid agreement, and the key elements of a mutual aid operational plan used for implementation. While

the NIMS guidance on mutual aid agreements does not provide legal authority or direction, it is intended to be used as a guideline for the development, revision, and synchronization of mutual aid agreements to ensure that jurisdictions can effectively integrate with one another prior to, during, and immediately following a large-scale incident. Any mutual aid discussions and agreements should be developed in accordance with existing Cal OES resource management processes

NIMS-Identified Types

- Local Automatic Mutual Aid
  - Agreements that permit the automatic dispatch and response of requested resources without incident-specific approvals. These may be formal or informal.
- Local Mutual Aid
  - Agreements between neighboring jurisdictions or organizations that involve a formal request for assistance. These agreements may cover a larger geographic area than automatic mutual aid agreements.
- Regional Mutual Aid
  - Sub-state, regional mutual aid agreements between multiple jurisdictions that are often sponsored by a council of governments or similar regional body.
- Intrastate/Statewide Mutual Aid
  - Agreements typically coordinated through the state that incorporate both state and local governmental and nongovernmental resources. These agreements help to reduce the number of local jurisdiction-to-jurisdiction mutual aid agreements.
- Interstate Mutual Aid – After Declaration
  - Out-of-state assistance as a result of formal State-to-State agreements through any number of vehicles. These vehicles may be interstate compacts and agreements, federal agreements, and/or sub-geographic pans. These mutual aid avenues may only be accessed after a formal emergency declaration. The type of declaration necessary is stipulated in the agreement.
- Interstate Mutual Aid – Prior to or Without a Declaration
  - Similar mechanisms as the Interstate Mutual Aid – After Declaration sections but may be accessed without a formal emergency declaration. In some instances, such as planned events, these agreements are especially necessary.

Mission Ready Packages

MRPs are resource packages developed by entities (resource providers) that reflect the entity's capacity to support affected jurisdictions during an incident through the sharing of resources. The MRP describes the resource's skills, limitations, support needed, and estimated costs.

MRPs can be developed for personnel resources, as well as equipment resources and provide potential resource providers with a way to succinctly describe their resource, including mission description, capability, resource footprint, limiting, and logistical support requirements, as well as develop valuable cost estimates, pre-event.

The most often used MRP template is used in regards tothe missions under the Emergency Management Assistance Compact (EMAC), but MRPs can be used to organize resource deploying under other means, as well.

The template consists of six tabs: MRP, Travel, Personnel, Equipment, Commodities, and Other. Each tab has its own purpose:

- MRP tab—Serves as a summary of the resource's capabilities, details, and estimate costs. It includes elements such as:
  - Resource provider information
  - Details on resource capabilities
  - Resource footprint and logistics support needed
  - Limitations
  - Cost estimate forms for travel, personnel, equipment, commodities, and other expenses are integrated into the workbook.
- Travel tab—The movement and billeting of mission resources including costs for freight to transport heavy equipment, flights, hotels, rental cars, and per-diem.
  - Travel costs for personnel (i.e. hotel, per-diem) should not be included as MRPs are not incident specific and any costs cannot be estimated accurately.
- Personnel tab—Salary, overtime, and fringe benefits for the number and type of personnel included in the resources.
  - Cost estimates should be based off a standard 14-day deployment plus two travel days.
  - Specific names and salary information should never be included. Agency or position salary averages should be captured instead.
- Equipment tab—Non-expendable resources that hold value after they have been used.
  - Costs to run equipment may be included (i.e. depreciation rate for its use).
    - List equipment even if there is no cost associated so that the Requesting State knows it is a part of the package and for documentation in case it is lost, stolen, or damaged.
    - Equipment purchased to conduct the mission that are included as an expense, are the property of the requesting state or jurisdiction and must be left with the requesting state or jurisdiction.
- Commodities tab—Expendable (or consumable) resources such as office supplies, water, ice, snacks, fuel, and other one-time-use items.

  - All receipts for commodities must be submitted at the time of reimbursement and must be directly related to the mission.
- Other Tab—Anything that does not fall under equipment or commodity such as mobile phone fees, laundry costs, decontamination, vaccination costs, equipment rentals, costs to restore equipment to pre-mission condition, and any other cost not specified elsewhere within the MRP form.

Completed MRPs are to be shared with the California EMAC Coordinator.

Federal Support

Federal law enforcement agencies can work with the State of California to address both criminal and national security cyber threats. These agencies, such as the FBI, U.S. Secret Service, and U.S. Immigration and Customs Enforcement, Homeland Security Investigations, can conduct threat response activities related to criminal activity involving their investigative jurisdictions.

- Department of Homeland Security (DHS)
  - Office of Cybersecurity and Communications
    - https://www.dhs.gov/office-cybersecurity-and-communications
  - National Cybersecurity and Communications Integration Center (NCCIC)
    - NCCIC@hq.dhs.gov
    - Phone: (888) 282-0870
  - United States Computer Emergency Readiness Team (US-CERT)
    - https://www.us-cert.gov/
- Federal Bureau of Investigation
  - iGuardian - The FBI's Industry-Focused Cyber Intrusion Reporting Platform
    - https://www.fbi.gov/resources/law-enforcement/iguardian
  - Internet Crime Complaint Center (IC3)
    - https://www.ic3.gov
  - Regional Cyber Task Force (Sacramento)
    - https://www.fbi.gov/contact-us/field-offices/sacramento
    - Phone: (857) 386-2000
- National Cyber Investigative Joint Task Force
  - cywatch@ic.fbi.gov
  - Phone: (855) 292-3937

- United States Immigration and Customs Enforcement/Homeland Security Investigations (ICE/HSI)
  - HSI Tip Line
    - https://www.ice.gov/webform/hsi-tip-form
    - Phone: (866) 347-2423
  - HSI Field Offices
    - https://www.ice.gov/contact/hsi
  - HSI Cyber Crime Center
    - https://www.ice.gov/cyber-crimes
- United States Secret Service
  - https://www.secretservice.gov/contact/field-offices/
  - Phone: (603) 626-5631