OCTOBER 2017

ACCELERATING THE CYBER INNOVATION ECONOMY

Cyber Center CCOE of Excellence

SAN DIEGO REGION-WIDE CYBER INCIDENT RESPONSE GUIDE

Regional Collaboration Powering Cyber Innovation

Developed in partnership with:

The City of SAN DIEGO
Office of Homeland Security

This plan was developed with input from representatives of the following Secure San Diego Stakeholders

AFCEA

AttackIQ

AUSGAR Technologies

Bank of America

Booz Allen Hamilton

CA Cyber Security Integration Center

CA Energy Commission

CA Governor's Military Council

CA Guard

CA State Threat Assessment Center

Cal State University San Marcos

CCOE

City of San Diego

CleanSpark

Cooley

CSI-SD

County of San Diego

CyberCalifornia

Defense Acquisition University

Diseño Communications

EDC

Ernst & Young LLP

ESET North America

FBI

FICO

iboss

Illumina

InfraGard San Diego

IOMAXIS

ISACA San Diego

KCD PR

Level 3 Communications

LevitZacks

Lockton Insurance

LP3

Marine Corps Installation West/Camp Pendleton

Morrison Foerster

Navy Region Southwest

Northrop Grumman

Port of San Diego

Protecting Tomorrow

Qualcomm

SANDAG

San Diego CISO Roundtable

San Diego County Regional Airport Authority

San Diego State University

Scientific Research Corp.

SD-LECC

SDMAC

Security Evaluators

Sempra Energy

Sentek Global

Sharp Healthcare

Securing Our eCity

SPAWAR

UC San Diego

University of San Diego

U.S. Air Force

U.S. Coast Guard

U.S. Secret Service

ViaSat

Webroot

PROMULGATION STATEMENT

Officials from the San Diego Cyber Center of Excellence, in conjunction with public and private sector stakeholders, have developed this Region-wide Cyber Incident Response Guide to enhance cyber emergency response capabilities and coordination throughout the San Diego region. This document is a result of that effort.

This guide is not directive or prescriptive, but rather is designed to promote coordination between private sector entities and public emergency services to maximize response effectiveness and minimize the effects of a cyber incident that may endanger life, property, and the environment. It incorporates the principles, processes, and standards set by the National Incident Management System (NIMS), CA Standardized Emergency Management System (SEMS), the Incident Command System (ICS), National Institute of Standards and Technology (NIST) Special Publication 800-61: Computer Security Incident Handling Guide, and the Federal Emergency Management Agency (FEMA) Comprehensive Preparedness Guide (CPG) 101 version 2.0

Government agencies, businesses, and non-governmental organizations have a public safety responsibility to respond to emergencies with minimal disruption to mission essential functions. This guide, when implemented throughout the region, will provide for better information sharing, forensics and investigations, and response to cybersecurity incidents. This guide is a living document that will be reviewed, updated, and exercise routinely and as necessary to adapt to the rapidly evolving landscape of cybersecurity.

As Co-Chair and President of the Cyber Center of Excellence, I give my full support of this guide and urge all public, private, and non-governmental organizations to coordinate internal cyber incident response plans with this guide to ensure consistency and coordination in cyber incident response.

Kenneth D Slaght

RADM (Ret.) Kenneth Slaght
Co-Chair & President
San Diego Cyber Center of Excellence

Table of Contents

I. Purpose / Mission

This cybersecurity response guide identifies procedures and responsibilities for private sector cyber incidents that require response capabilities greater than the affected company, as well as cooperative efforts with local government agencies.

A. Strategies and Goals

Ensure effective response to cybersecurity incidents, protect organization data from loss, and prevent further disruption of operations.

B. Whole Community Approach

The whole community concept is a process by which residents, emergency management representatives, organizational and community leaders, and government officials can understand and assess the needs of their respective communities and determine the best ways to organize and strengthen their resources, capacities, and interests. Engaging in whole community emergency management planning builds a more effective path to societal security and resilience. This annex supports the following whole community principles:

- Understand and meet the needs of the entire community, including people with disabilities and those with other access and functional needs.
- Engage and empower all parts of the community to assist in all phases of the disaster cycle.
- Strengthen what works well in communities on a daily basis.

This guide was developed with the guidance of representatives from the cybersecurity community, law enforcement, emergency management, access and functional needs communities, and various other stakeholders. The effectiveness of the emergency response is largely predicated on the preparedness and resiliency of the community.

C. Senior Management Approval

Each organization should have a formal, focused, and coordinated approach that is supported by senior management for responding to incidents.

D. Planning Assumptions

Assumptions indicate areas where adjustments to this Annex may be needed as the facts of the incident become known. The following assumptions were made in developing this Annex:

- In the event of a large cyber incident that endangers health, life, or property, the incident will be reported to 9-1-1 and the City's Emergency Operations Center may be activated to coordinate resources from local, state, and federal agencies.
- A cyber-related emergency may take many forms, such as: virus outbreak; server compromise; data breach; denial of service attacks; service-impacting incidents caused by security device, server, or application issues; and other critical incidents that have negative impact on confidentiality, availability, or integrity of applications, computing infrastructure, or data.

- A cyber-related emergency may cause complete and immediate work stoppage affecting a primary business process or broad group of employees
- A cyber-related emergency may threaten lives, property, the economy, or national security
- A workaround may not be available, or may be available but not easily sustainable
- Security incidents less severe in nature will be handled by individual company or office protocols
- A breach may occur without data yet being exploited or a clear initial indication

E. Policies and Guidelines

- All suspected or confirmed computer security incidents will be subject to reporting requirements
- Discussion of incident information with outside parties shall only be done in accordance with the affected company's policies; no company information will be shared without prior authorization from the affected company.

II. Concept of Operations and Organizational Approach

A. Activation

This Annex is activated during an emergency that exhausts the resources of one company and upon request for activation by the Incident Commander.

B. Organization and Assignment of Responsibilities

i. Central Incident Response Team

The Central Incident Response Team consists of employees and contractors of the affected company who regularly conduct cybersecurity activity. The Central Incident Response Team will follow all established plans, policies, and protocols developed by their company.

a. Response Planning, Communications, and Analysis

In an expanding or compounding incident, the team shall designate an Incident Commander to provide direction and contain and/or mitigate damage. Response processes and procedures are to be executed and maintained to ensure timely response to detected cybersecurity events. Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from local government agencies. Analysis is conducted to ensure adequate response and recovery activities.

- □ Triage and confirm the incident(s)
- □ Investigate notifications from detection systems and situational awareness systems and determine the Traffic Light Protocol (TLP) level for information sharing and Security Risk Level per Table 1 and 2. For additional information on TLP standards, see Attachment B: Traffic Light Protocols.
- □ Document the investigation and actions taken

- □ Preserve evidence for forensic investigations, damage assessments, and impact assessments, such as source of the breach and details of systems affected
- □ Implement filtering based on the characteristics of the attack, if feasible
- □ Contact the ISP for assistance in filtering the attack, if applicable
- □ Report suspected or actual cyber events to fulfill mandatory reporting requirements, per Attachment A: San Diego Cyber Incident Reporting & Resource Map.
- □ For incidents with cascading impacts that endanger life or property, notify the appropriate local authorities as soon as possible to limit further damage. Imminent threats to life or property should be reported by calling 9-1-1. This will trigger the activation of the agency's Emergency Operations Center (EOC), if warranted. The incident report should include:
  - o Type of cyber incident (firewall breach, network attack, etc.)
  - o Incident assessment (damage, cascading effects, etc.)
  - o Expected duration of the incident (if possible)
  - o Any additional information to help determine appropriate level of government response
- □ Provide information for public messaging to the organization's media personnel and local government agency EOC, if activated.

Table 1: Traffic Light Protocol (TLP)

Priority	Definition
TLP:RED ● ○ ○ Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. The problem has caused Personal Identifiable Information (PII) or other critical data to be exfiltrated and/or has caused complete and immediate work stoppage affecting a primary business process or a broad group of End Users such as an entire department, floor, branch, line of business, or external customer. No workaround is available.

TLP:AMBER ○🟠○ Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. A business process is affected in such a way that business functions are severely degraded, multiple End Users are impacted or a key customer is affected. Workaround may be available or not easily sustainable.
TLP:GREEN ○○🟢 Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. A business process is affected in such a way that certain functions are unavailable to End Users or a system and/or service is degraded. A workaround may be available.
TLP:WHITE ⚪⚪⚪ Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.

Table 2: Security Risk Levels

Severity	Definition
High	Risk discovered on internet-facing device or wireless network infrastructure where device compromise, unauthorized access, or degraded performance is likely to occur in a short period of time. Risk discovered due to access to PII by unauthorized personnel, unauthorized access to financial data, or data seemed sensitive and not for public consumption, whether internal-facing or not.
Medium	Risk discovered on critical infrastructure system or on systems that contain client sensitive data where infrastructure is highly susceptible to device compromise or unauthorized access.

b. Response Mitigation

- □ Confirm containment of the event
- □ Inform networked partners and stakeholders of suspected and confirmed cyber incidents and breaches, and develop and submit event reports and situation impact assessments to stakeholders, per the organization’s reporting requirements and processes.
- □ Upon EOC activation by a government entity, coordinate cyber event response activities and resource requests through the EOC.
- □ Mitigate newly identified vulnerabilities or document accepted risks.
- □ Identify and mitigate all vulnerabilities that were exploited.

c. Improvements

- □ Develop and publish a cyber event After Action Report/Improvement Plan (AAR/IP), per organizational requirements
- □ If an EOC was activated, submit After Action Report/Improvement Plan (AAR/IP) to the local government agency EOC for consolidation of relevant items, lessons learned, and information into a regional reference.
- □ Update and exercise response plans and strategies. See III.B. Incident Response Capability Development and Maintenance

ii. Local Government Agency

□ Determine level of EOC activation and activate per agency protocols, if necessary

□ Receive situation reports from the organization's Central Incident Response Team.

□ Conduct emergency response efforts per the agency/jurisdiction Emergency Operations Plan and other relevant plans, protocols, and procedures.

□ Determine if a proclamation of a local emergency is necessary, and coordinate with Operational Area EOC and other stakeholders. See Attachment C: Incident Flow Chart.

□ Coordinate resources and information with other local government entities, and state and federal government entities as needed.

□ Coordinate public information messaging with the organization's media personnel.

C. Capability Metrics

Capability Metrics should be compiled for every incident for organizational situational awareness, per Table 3.

Table 3

Capability Metrics Guidance

Category	Measurement	Description
Incidents	# Total Incidents / Year	Total amount of incidents responded to per year
	# Incidents by Type / Year	Total number of incidents by category responded to per year
Time	# Personnel Hours / Incident	Total amount of labor spent resolving incident
	# Days / Incident	Total amount of days spent resolving incident
	# System Down-Time Hours / Incident	Total hours of system down-time until incident resolved
Cost	Estimated Monetary Cost / Incident	Total estimated monetary cost per incident, to include containment, eradication, and recovery, as well as collection & analysis activities (this may include labor costs, external entity assistance, tool procurements, travel, etc.)
Damage	# Systems Affected / Incident	Total number of systems affected per incident
	# Records Compromised / Incident	Total number of records compromised per incident
Forensics	# Total Forensics Leveraged Incidents / Year	Total number of incidents requiring forensics (collection & analysis) per year
	# System Images Analyzed / Incident	Total number of system images analyzed per incident
	# System Memory Dumps Examined / Incident	Total number of system physical memory dumps examined per incident

III. Administration, Finance, and Logistics

A. Vital Records Retention and Preservation

All records related to the cyber incident shall be retained by the affected company, other than those required by law to be retained or preserved by a government agency. Company documents shall not be distributed unless prior authorization is received from the affected company.

B. Incident Response Capability Development and Maintenance

The City of San Diego Office of Homeland Security is responsible for coordinating the update, training, and exercise of this guide per the schedule listed in Table 3. San Diego regional stakeholders will support and participate in update, training, and exercise of this guide. San Diego regional stakeholders will develop, update, train, and exercise their organization-specific plans, processes, and procedures that support and interoperate with this guide.

Table 4

Region-wide Cyber Incident Response Guide
Maintenance and Exercise Schedule

Activity	Specific Task	Responsible Party	Frequency
Review of Region-wide Cyber Incident Response Guide	Review entire Region-wide Cyber Incident Response Guide for accuracy Annotate any changes in content, information, and policy Submit changes to the Cyber Center of Excellence or confirm that no changes are required	CCOE, City of San Diego Office of Homeland Security	Annually, by January 31
Update of Region-wide Cyber Incident Response Guide	Incorporate changes as submitted by the Cyber Center of Excellence membership Publish / Distribute updated Cybersecurity Response Guide	City of San Diego Office of Homeland Security	Annually, by February 28
Exercise of Region-wide Cyber Incident Response Guide	Conduct a Region-wide Cyber Incident Response Guide exercise	City of San Diego Office of Homeland Security All Stakeholders	Annually, by September 30

C. Authorities and References

- The Federal Information Security Modernization Act of 2014 (FISMA)
- National Institute of Standards and Technology Special Publication 800-86 *Guide to Integrating Forensic Techniques into Incident Response*, August 2006
- U.S. Department of Homeland Security *National Incident Management System*, December 2008
- FEMA, *Comprehensive Preparedness Guide (CPG) 101, Version 2.0*, November 2010
- Health Insurance Portability and Accountability Act (HIPPA)
- Presidential Policy Directive 21: *Critical Infrastructure Security and Resilience,* 2013
- California Civil Code 1798.29, *Information Practices Act of 1977*
- California *Standardized Emergency Management System*, November 2009
- Unified San Diego County Emergency Services Organization, *Cyber Disruption Response Planning Annex*, September 2015
- City of San Diego Municipal Code Chapter 5, Article 1, Division 1, *Public Emergency Procedures*, April 2016
- City of San Diego Administrative Regulation 1.01, *Emergency Operations Procedures*, October 2010
- City of San Diego *Emergency Operations Plan*, March 2011
- City of San Diego Department of IT *Incident Response Guidelines,* June 2016
- City of San Diego Department of IT *Information Security Standards and Guidelines,* June 2016
- Security Standards Council, *Payment Card Industry Data Security Standard,* April 2016

ATTACHMENT A: San Diego Cyber Incident Reporting & Resource Map

GENERAL INCIDENT REPORTING GUIDANCE & RESOURCES

Cybersecurity reporting laws and requirements are constantly changing; this is meant to be a guide for incident reporting, and legal advice should be sought for incident response.

Local Government Response Agency

Cyber incidents that have large cascading effects that result in imminent danger to life or property (e.g. chemical releases, damage to critical infrastructure) should be reported to local authorities by calling 9-1-1.

Expected Response: If the cyber incident causes a large-scale emergency, the City's Emergency Operations Center may be activated in order to coordinate all local, State, and federal resources.

State of California

Any breach that involves personal information must be reported to the affected California residents. Data breaches that affect 500 or more Californians must also be reported to the California Attorney General https://oag.ca.gov/ecrime/databreach/reporting.

Additionally, if social security, driver's license, or state identification card numbers are breached, and the entity providing notice was the source of the breach, the entity must provide identity theft prevention and mitigation services at no cost to affected parties for at least 12 months.

Expected Response: The Attorney General will follow up with the reporting entity if additional information is needed. Data breaches reported will be posted on the Office of the Attorney General website.

Department of Justice – FBI Internet Crime Complaint Center (IC3)

Cybercrime, including computer intrusions or attacks, password trafficking, fraud, violation of federal statutes, intellectual property theft, identity theft, theft of trade secrets, child pornography, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity: https://www.ic3.gov/complaint

Expected Response:
The incident will be logged; based on severity, the FBI may follow-up via phone.

Department of Homeland Security: National U.S. Computer Emergency Readiness Team (US-CERT)

Suspected or confirmed cyber incidents that may impact critical infrastructure and require technical response and mitigation assistance: https://www.us-cert.gov/forms/report

Expected Response: US-CERT will log the information for the national database and send confirmation of receipt to the reporting entity. Resources may be deployed if all local and State resources are exhausted.

AEROSPACE & UNMANNED SYSTEMS

Since Lindbergh's Spirit of St. Louis, San Diego has been at the core of historic aerospace advances and continues to serve as a worldwide leader in aviation. Now evolving to include unmanned systems in addition to traditional aircraft, the aerospace industry provides more than 85,000 jobs and $39.9 billion in output to the local economy. San Diego's aviation innovators are developing tomorrow's technologies and continuing the region's legacy today.

Cybersecurity Incident Reporting & Expected Response: Aircraft that experience accidents or incidents due to cyber breaches must follow traditional accident and incident reporting requirements with NASA's Aviation Reporting System, the National Transportation Safety Board, and the Federal Aviation Administration for traditional and unmanned aircraft systems.

Corresponding DHS Sectors: Critical Manufacturing, Defense Industrial Base, Transportation

CLEANTECH

San Diego has installed more solar power than any other major American City, the region is embracing wind and other alternative energy solutions, and the San Diego Climate Action Plan sets a goal to cut carbon production in half by 2035. The region's clean technology cluster not only makes these goals feasible, but makes San Diego an international leader in renewable energy solutions.

Cybersecurity Incident Reporting & Expected Response:
The Department of Energy requires DOE contractors to report cyber incidents to the Joint Cybersecurity Coordination Center (JC3). Incidents should be reported via internet at https://tickets.ijc3.doe.gov. Additionally, the JC3 Call Center is available 24/7 at 866-941-2472 for after-hours emergencies and incidents involving classified computer systems. The Department of Energy may provide assistance if local and state resources are exhausted, per the National Incident Management System.

Corresponding DHS Sector: Energy, Critical Manufacturing

COMMUNICATIONS & TECHNOLOGY

From wireless technology development and computer programming to engineering services and electronic instrument manufacturing, San Diego is home to some of the brightest minds in the nation. The Communications & Technology sector develops solutions that keeps San Diego connected.

Cybersecurity Incident Reporting & Expected Response: There are no unique reporting requirements for this sector.

Corresponding DHS Sectors: Communications, Information Technology

CRAFT GOODS

San Diego has quickly emerged as the "Capital of Craft" due to its thriving craft beer, juice, food industries; its world renowned instruments; and other unique San Diego goods. The 13% employment increase in San Diego craft goods over the last five years makes this one of the most rapidly growing industries in the region.

Cybersecurity Incident Reporting & Expected Response: There are no unique reporting requirements for this sector.

Corresponding DHS Sector: Commercial Facilities, Food and Agriculture

DEFENSE

San Diego receives more defense spending than nearly any other county in the nation, with over $8 billion in contracts between the federal government and San Diego companies in 2016 and a projected 4.3% increase in 2017. With the nation's more pressing national security projects being developed in San Diego, cybersecurity is exceedingly important for this industry.

Cybersecurity Incident Reporting & Expected Response:
Report via DIBNet (http://dibnet.dod.mil) and complete the Incident Collection Form. If you are a subcontractor, you must also report cyber incidents to the prime contractor – provide the DIBNet incident report number as soon as practicable, along with any other information required by the prime contractor. The reporting entity will receive an email back confirming the report has been received, and the Department of Defense may request access to information or equipment for forensic analysis and damage assessment. Depending on the contract, there may be requirements to report to the Department of Defense Security Service (DSS), per contract reporting procedures. The response may vary based on the contract.

Corresponding DHS Sectors: Critical Manufacturing, Defense Industrial Base

EDUCATION

San Diego's six universities and more than 80 research institutes conduct groundbreaking research, train the region's workforce, and provide a workforce and technology infrastructure that enables the region to compete for investment and jobs on a global level.

Cybersecurity Incident Reporting & Expected Response: If student financial aid information is involved, a breach report must be filed with the U.S. Department of Education. Title IV schools must report on the day of detection when a data breach is even suspected. Incident details should be reported to cpssaig@ed.gov and include breach information and a list of your data-breach team and executives. If email is unavailable, reports can be made to the Education Security Operations Center at 202-245-6550. The Department of Education may follow up, depending on the severity of the incident.

Corresponding DHS Sectors: Government Facilities

FINANCIAL SERVICES

The financial services sector has grown to meet the modern demands of instant access to funds and money management. With new technologies constantly onboarding to improve customer satisfaction and the vast amount of personally identifiable information, strong cybersecurity measures are necessity for a successful financial services organization.

Cybersecurity Incident Reporting & Expected Response:
National banks are required to report intrusions and other computer crimes to the Department of the Treasury via the Office of the Comptroller of Currency:
http://bsaefiling.fincen.treas.gov/main.html
If a cyber incident affects a payment system, a report should also be made to the U.S. Secret Service by calling 619-557-5640. Depending on the severity of the incident, the Secret Service may deploy resources to conduct a forensic investigation. Federal law also requires notice be issued to all customers affected. In cases where financial institutions recommend a large number of affected clients to request fraud alerts and credit freezes for their files, the Federal Trade Commission (FTC) advises the institution to notify the major credit bureaus.

Corresponding DHS Sectors: Commercial Facilities, Financial Services

HEALTHCARE

San Diego's diverse academic and clinically-focused medical centers and hospitals solidify San Diego's place as a nationwide leader in healthcare. San Diego's healthcare industry is responsible for direct employment of 140,000 people and $6.9 billion in wages annually.

Cybersecurity Incident Reporting & Expected Response:
HIPAA requires breaches to be reported to the U.S. Secretary of Health and Human Services (HHS); HHS requires this notice to be completed through their online portal:
https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html
Additionally, the HIPPA Breach Notification Rule requires breaches affecting more than 500 residents of a State or jurisdiction be reported to prominent media outlets serving the State or jurisdiction.

The California Department of Health Care Services Office of HIPAA Compliance must be notified within 15 days of the breach via phone or email:
(916) 445-4646, (866) 866-0602, or privacyofficer@dhcs.ca.gov

For companies that provide online personal health care record management, the Federal Trade Commission (FTC) requires breached companies to complete a "Notice of Breach of Health Information," which can be found here:
https://www.ftc.gov/system/files/documents/plain-language/2017_5_2_breach_notification_form.pdf

Corresponding DHS Sectors: Healthcare and Public Health

HOSPITALITY & TOURISM

San Diego is a top U.S. travel destination, hosting more than 34.9 million visitors each year. Visitors spend nearly $10.4 billion annually at San Diego businesses and produce $267 million in transient occupancy tax revenues. With targeted attacks on the hospitality industry growing, it is essential that this sector is prepared.

Cybersecurity Incident Reporting & Expected Response: If a cyber incident affects a payment system, a report should also be made to the U.S. Secret Service by calling 619-557-5640.

Corresponding DHS Sectors: Commercial Facilities

LIFE SCIENCES

The San Diego Life Sciences sector is responsible for over 1,100 life science companies and more than $31.8 billion in total economic impact to the region. San Diego's 11 million square feet of lab space and 7,000 annual STEM graduates fuels breakthrough technologies that make San Diego one of the top life sciences markets in the world.

Cybersecurity Incident Reporting & Expected Response: If conducting research and development on behalf of an organization, refer to contract for reporting and response protocols.

Corresponding DHS Sectors: Chemical, Healthcare and Public Health

MARITIME

With a world-class port and 70 miles of coastline, San Diego is the ideal location for the "Blue Economy." The Blue Economy includes fishing, ship building, port construction, and maritime technology and employs approximately 46,000 San Diegans.

Cybersecurity Incident Reporting & Expected Response: For manufacturing as a contractor of the Department of Defense, please see the "Defense" section. Facility and vessel operators must report to the National Response Center (NRC) at 1-800-424-8802. Report the incident to US-CERT and note in your report that you are a Coast Guard regulated entity. Transportation incidents should also be reported to the National Transportation Safety Board at 1-844-373-9922. Agencies will follow up with the reporting entity for investigation.

Corresponding DHS Sectors: Critical Manufacturing, Defense Industrial Base

MANUFACTURING

San Diego's manufacturing sector is diverse, and is inclusive of several manufacturing clusters: biotech, cleantech, defense and security, electronics and telecommunications, and food and beverage production. With the average manufacturing worker's wage at $81,180 in 2016 and employing 105,782 people in 2016, the manufacturing cluster is at the core of our regional economy.

Cybersecurity Incident Reporting & Expected Response: For manufacturing as a contractor of the Department of Defense or Department of Energy, please see the "Cleantech" and "Defense" sections.

Corresponding DHS Sectors: Chemical, Communications, Critical Manufacturing, Defense Industrial Base

SPORTS & ACTIVE LIFESTYLE

The beautiful weather and unparalleled landscape make San Diego the ideal place for the sports and active lifestyle industry. This unique industry accounts for $1.4 billion in regional economic activity, employs 23,000 people, and keeps San Diego on the list of go-to vacation spots for visitors from around the world.

Cybersecurity Incident Reporting & Expected Response: If a cyber incident affects a payment system, a report should also be made to the U.S. Secret Service by calling 619-557-5640.

Corresponding DHS Sectors: Commercial Facilities, Critical Manufacturing

TRANSPORTATION

As one mega-region, the San Diego-Tijuana economies are closely related and depend on reliable transportation to succeed. Land, sea, and air transportation allow the region's innovation and creativity to be shared with the world. The transportation sector literally keeps San Diego's economy moving.

Cybersecurity Incident Reporting & Expected Response: Transportation incidents should be reported to the National Transportation Safety Board (NTSB) at 1-844-373-9922. NASA Aviation Safety Reporting system

Corresponding DHS Sectors: Transportation Systems

UTILITIES

Utility providers supply fuel to the transportation sector, power homes across the nation, and ensure safe drinking water. Utilities play a role in every other sector, and therefore, strong cybersecurity practices in this sector are vital to the success of the economy as a whole.

Cybersecurity Incident Reporting & Expected Response:
The Department of Energy requires DOE contractors to report cyber incidents to the Joint Cybersecurity Coordination Center (JC3). Incidents should be reported via internet at https://tickets.ijc3.doe.gov. The California Public Utilities Commission requires reporting of certain incidents at http://www.cpuc.ca.gov/emrep/. Incidents at nuclear facilities must be reported to the NRC Operations Center at (301) 816-5100.
Oil, Gas, or Geothermal operators must report to the California Department of Conservation http://www.conservation.ca.gov/dog/Pages/doggr_contacts.aspx

Corresponding DHS Sectors: Dams; Energy; Nuclear Reactors, Materials, and Waste; Water and Wastewater Systems

RESOURCES AVAILABLE

- Training & Information Sharing:
  - InfraGard San Diego
    InfraGard is a FBI-affiliated non-profit that works to mitigate criminal and terrorist threats, risks, and losses, for the purpose of protecting the region's critical infrastructure and the American people.
    http://www.infragardsd.org/
  - In-person training for emergency management is offered through the San Diego Regional Training Program; open to all with a security role: https://sduasi.org/
  - DHS Federal Virtual Training Environment (FedVTE); training for Government Personnel, Government Contractors, and U.S. Veterans: https://fedvte.usalearning.gov/

- FEMA Emergency Management Institute Independent Study Program; open to all: https://training.fema.gov/is/
- Newsletters and publications are available to members of the Cyber Center of Excellence (CCOE), a non-profit dedicated to accelerating the region's cyber economy and positioning https://sdccoe.org/publications/
- Agencies including the FBI, Department of Administrative Services (DAS), Office of Homeland Security (OHS), and San Diego Police Department (SDPD) may also provide training and information sharing opportunities, such as the FBI Cyberhood Watch Program.

ATTACHMENT B: Traffic Light Protocol (TLP) Definitions and Usage

This information is provided by US-CERT for standard definition and usage guidance.

The Traffic Light Protocol (TLP) was created in order to facilitate greater sharing of information. TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colors to indicate expected sharing boundaries to be applied by the recipient(s). TLP only has four colors; any designations not listed in this standard are not considered valid by FIRST.

TLP provides a simple and intuitive schema for indicating when and how sensitive information can be shared, facilitating more frequent and effective collaboration. TLP is not a "control marking" or classification scheme. TLP was not designed to handle licensing terms, handling and encryption rules, and restrictions on action or instrumentation of information. TLP labels and their definitions are not intended to have any effect on freedom of information or "sunshine" laws in any jurisdiction.

TLP is optimized for ease of adoption, human readability and person-to-person sharing; it may be used in automated sharing exchanges, but is not optimized for that use.

TLP is distinct from the Chatham House Rule (when a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.), but may be used in conjunction if it is deemed appropriate by participants in an information exchange.

The source is responsible for ensuring that recipients of TLP information understand and can follow TLP sharing guidance.

If a recipient needs to share the information more widely than indicated by the original TLP designation, they must obtain explicit permission from the original source.

DEFINITIONS

Color	When should it be used?	How may it be shared?
TLP:RED ●○○	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER	Sources may use TLP:AMBER when	Recipients may only share

○●○	information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
TLP:GREEN ○○●	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE ○○○	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

USAGE

How to use TLP in email

TLP-designated email correspondence should indicate the TLP color of the information in the Subject line and in the body of the email, prior to the designated information itself. The TLP color must be in capital letters: TLP:RED, TLP:AMBER, TLP:GREEN, or TLP:WHITE.

How to use TLP in documents

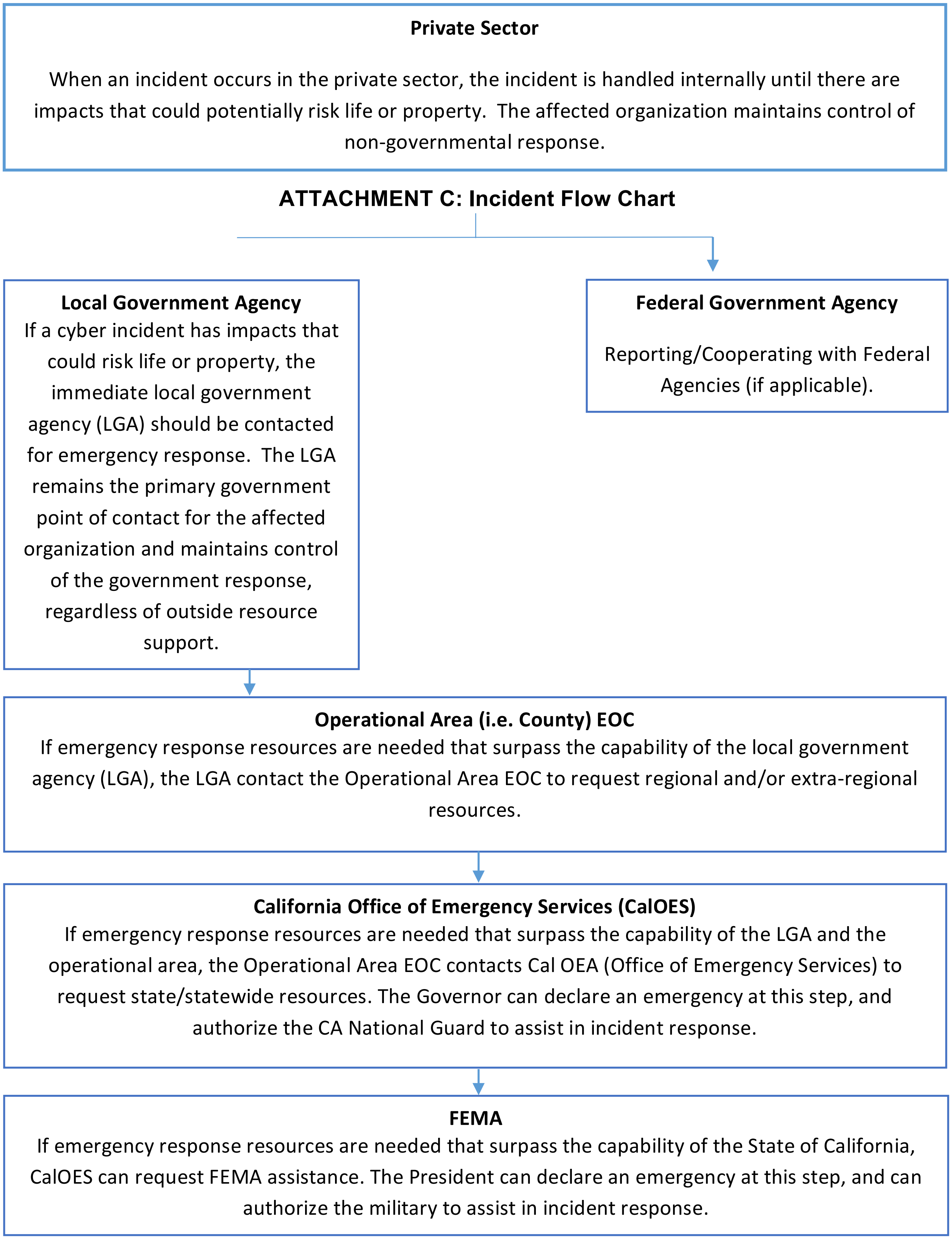
TLP-designated documents should indicate the TLP color of the information in the header and footer of each page. To avoid confusion with existing control marking schemes, it is advisable to right-justify TLP designations. The TLP color should appear in capital letters and in 12 point type or greater.

RGB:
TLP:RED : R=255, G=0, B=51, background: R=0, G=0, B=0
TLP:AMBER : R=255, G=192, B=0, background: R=0, G=0, B=0
TLP:GREEN : R=51, G=255, B=0, background: R=0, G=0, B=0
TLP:WHITE : R=255, G=255, B=255, background: R=0, G=0, B=0

CMYK:
TLP:RED : C=0, M=100, Y=79, K=0, background: C=0, M=0, Y=0, K=100
TLP:AMBER : C=0, M=25, Y=100, K=0, background: C=0, M=0, Y=0, K=100
TLP:GREEN : C=79, M=0, Y=100, K=0, background: C=0, M=0, Y=0, K=100
TLP:WHITE : C=0, M=0, Y=0, K=0, background: C=0, M=0, Y=0, K=100

(Concurrent Actions)

ATTACHMENT C: Incident Flow Chart



Private Sector

When an incident occurs in the private sector, the incident is handled internally until there are impacts that could potentially risk life or property. The affected organization maintains control of non-governmental response.

Local Government Agency

If a cyber incident has impacts that could risk life or property, the immediate local government agency (LGA) should be contacted for emergency response. The LGA remains the primary government point of contact for the affected organization and maintains control of the government response, regardless of outside resource support.

Federal Government Agency

Reporting/Cooperating with Federal Agencies (if applicable).

Operational Area (i.e. County) EOC

If emergency response resources are needed that surpass the capability of the local government agency (LGA), the LGA contact the Operational Area EOC to request regional and/or extra-regional resources.

California Office of Emergency Services (CalOES)

If emergency response resources are needed that surpass the capability of the LGA and the operational area, the Operational Area EOC contacts Cal OEA (Office of Emergency Services) to request state/statewide resources. The Governor can declare an emergency at this step, and authorize the CA National Guard to assist in incident response.

FEMA

If emergency response resources are needed that surpass the capability of the State of California, CalOES can request FEMA assistance. The President can declare an emergency at this step, and can authorize the military to assist in incident response.

ACCELERATING THE CYBER INNOVATION ECONOMY

Cyber Center
CCOE
of Excellence

Rear Admiral Ken Slaght, USN, Retired
CCOE Co-Chair and President

Lisa Easterly
CCOE Chief Operating Officer

Cyber Center of Excellence
610 West Ash Street, Suite 701
San Diego, CA 92101

www.sdccoe.org
info@sdccoe.org

in @sdccoe