INCIDENT RESPONSE

Donald E. Hester
CISA Cybersecurity Advisor – San Francisco Bay Area
Cybersecurity Advisor Program
Cell: +1 (202) 315-8091
Email: donald.hester@cisa.dhs.gov

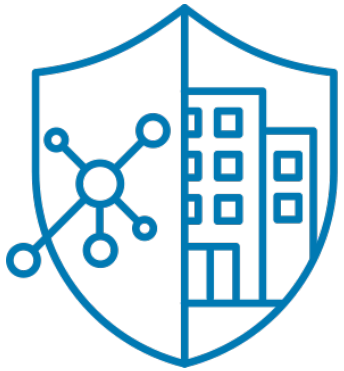
Jake Aguiar
CISA Cybersecurity Advisor – Orange County, CA
Cybersecurity Advisor Program
Cell: +1 (202) 957-3040
Email: jacob.aguiar@cisa.dhs.gov

CISA.IOD.REGION.R09_Ops@cisa.dhs.gov

WHO WE ARE

CISA Mission and Vision

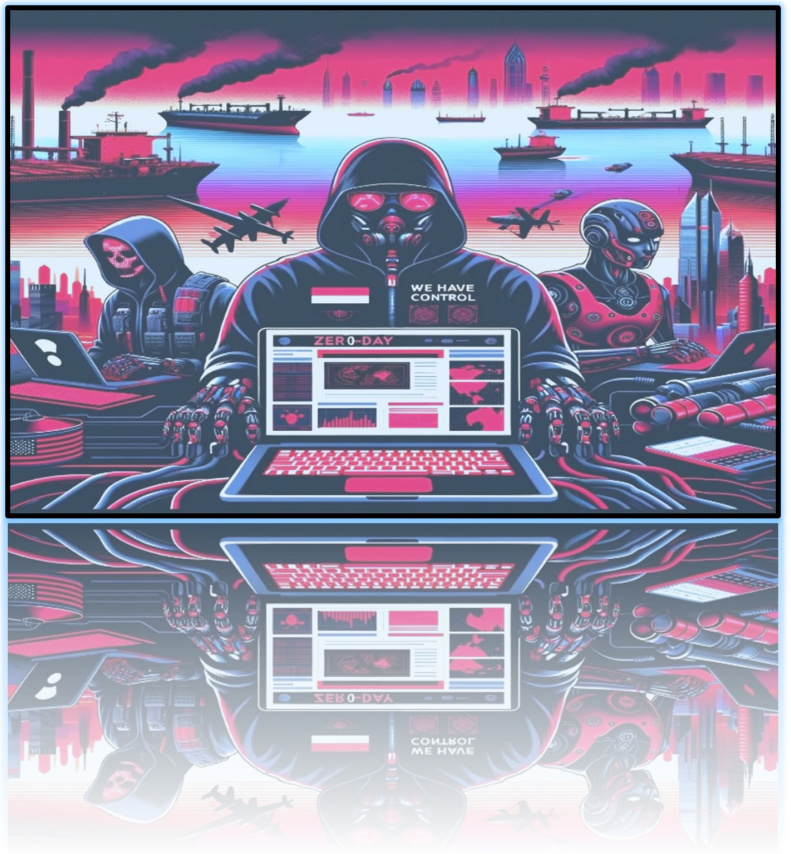
- Cybersecurity and Infrastructure Security Agency (CISA) mission:
  - Lead the collaborative national effort to strengthen the security and resilience of America's critical infrastructure
- CISA vision:
  - A Nation with secure, resilient, and reliable critical infrastructure upon which the American way of life can thrive



Current Situation

Cyber Threats

- Ransomware
- Malware
- Advanced Persistent Threats (APT)
- DDoS
- Threat to External Dependencies
- Social Engineering



Cryptojacking

Collateral Damage

Destruction

Ransom

Data Theft

All of the Above

Donald E. Hester
March 19, 2024

Threat Actors

- Most Cyber-criminals look for ways to make money.
- Some want to make a statement.
- Some just want destruction.

Donald E. Hester
March 19, 2024

Warning

- “China’s hackers are positioning on American infrastructure in preparation to wreak havoc and cause real-world harm to American citizens and communities, if or when China decides the time has come to strike”
- “Cyber threats to our critical infrastructure represent real world threats to our physical safety.”
- Wray told the House Select Committee on the Chinese Communist Party.

General Paul Nakasone, Commander, United States Cyber Command
Ms. Jen Easterly, Director, Cybersecurity and Infrastructure Security Agency
Mr. Christopher Wray, Director, Federal Bureau of Investigation
Mr. Harry Coker, Jr., Director, Office of the National Cyber Director

https://selectcommitteeontheccp.house.gov/committee-activity/hearings/hearing-notice-ccp-cyber-threat-american-homeland-and-national-security (31 JAN 2024)

AI Threats

- Attacking AI Systems
- AI Enabled Phishing
- AI Enabled Vulnerability Research
- AI Enabled Hacking
- Disinformation

Donald E. Hester
March 19, 2024

Cyber Incident Response

NIST Cybersecurity Framework (CSF)

- This voluntary Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk.
- The Cybersecurity Framework's prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security.

Donald E. Hester
March 19, 2024

NIST Cybersecurity Framework (CSF)

Framework Core Functions

RECOVER

Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

RESPOND

Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

IDENTIFY

Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

PROTECT

Develop and implement appropriate safeguards to ensure delivery of critical services.

DETECT

Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

Using the NIST CSF

Identify

- Inventory tools
- Asset Management
- Risk Assessment
- Governance
- Business Goals

Protect

- Awareness
- Maintenance
- Vulnerability Management
- Configuration Management
- Data Security
- Protective Technologies
- Access Control

Detect

- Intrusion Detection
- Endpoint Detection and Response
- Data Leak Protection
- Security information and event management
- Threat Intelligence

Respond

- Endpoint Detection and Response
- Intrusion Prevention
- Security orchestration, automation, and response
- Table-Top Exercise

Recover

- Backups
- Business Continuity
- After Action
- Communication

Donald E. Hester
March 19, 2024

Cyber Incident Response Plan Contents

- Purpose
- Scope
- Policy
- Cyber-Incident Response Team (CIRT)
  - Roles & Responsibilities
- Definitions
- Preparation and Planning
- Detection and Analysis
- Escalation
- Containment, Eradication, and Recovery
- Post Incident Activities
- Cyber Incident Response Reference

Related Plans

- Cyber Incident Response Plan
- Disaster Recovery Plan
- Business Continuity Plan
- Emergency Communications Plan
- Emergency Operations Plan
- Continuity of Operations Plan

- Thes plans are all critical components of an organization's overall risk management strategy.
- While each plan has a unique focus, they are all interrelated and work together to ensure the organization can continue to operate in the face of unexpected disruptions.

Developing a Plan

Emergency Operations Six-Step Planning Process
Planning Considerations for Cyber Incidents, Guidance for Emergency Managers, Nov 2023
FEMA / CISA

Define Impact

Sensitive Cybersecurity Information

Prioritization

Prioritization should be based on the impact to City business functions and information sensitivity.

- Functional impact, impact to City's mission, public safety, recoverability, information sensitivity, and fiscal impact
- Impact may affect confidentiality, integrity, or availability of City information
- Size of the incident, widespread or localized
- Amount of downtime before recovery
- Impact to City reputation

Sample

Business Function Impact

- **No Impact**: No effect on the City's ability to provide all services to all users
- **Low Impact**: Minimal effect; the City can still provide all critical services to all users but has lost efficiency
- **Moderate Impact**: The City has lost the ability to provide a critical service to a subset of system users
- **High Impact**: The City is no longer able to provide some critical services to any users

Information Sensitivity Impact

- **None**: No information was exfiltrated, changed, deleted, or otherwise compromised
- **Privacy Breach**: Sensitive information was accessed or exfiltrated
- **Proprietary Breach**: Proprietary information was accessed or exfiltrated
- **Integrity Loss**: Sensitive or proprietary information was changed or deleted
- **Availability Loss**: Sensitive or proprietary information was unavailable or inaccessible

Severity Determination

Severity Determination

The City will use the Cyber Incident Severity Matrix from Cal OES CA-ESF 18 Annex to rate the severity Cyber Incident.

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.

CalOES ESF 18

Severity and Activation

CalOES ESF 18

Severity and Activation

The City will use the Cyber Activation Level from Cal OES CA-ESF 18 Annex.

California Cyber Incident Severity	Activation Level	Description
Level 0 Steady State	N/A	N/A
Level 1 Low	Level 3	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 2 Medium		
Level 3 High	Level 2	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 4 Severe		
Level 5 Emergency	Level 1	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.

Containment, Eradication, and Recovery

- Containment
- Evidence Collection
- Eradication
- Recovery
- Recovery Severity
- Execution of Business Continuity Plans
- Execution of Disaster Recovery Plans

- **Regular:** Time to recovery is predictable with existing resources
- **Supplemented:** Time to recovery is predictable with additional resources
- **Extended:** Time to recovery is unpredictable; additional resources and outside help are needed
- **Not Recoverable:** Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly)

Post Incident Activities

- Reporting Cyber-Incidents
- After Action Meeting
- After Action Report
- External Reporting
- Evidence Retention
- Quality Assurance and Follow-up

- Sheriff's Office
- California Department of Justice (CLETS)
- Department of Justice (CJIS)
- Merchant Bank (PCI)
- U.S. Department of Health & Human Services (HIPAA)
- ISACs
- CISA (CIRCIA)

Incident Response Resources

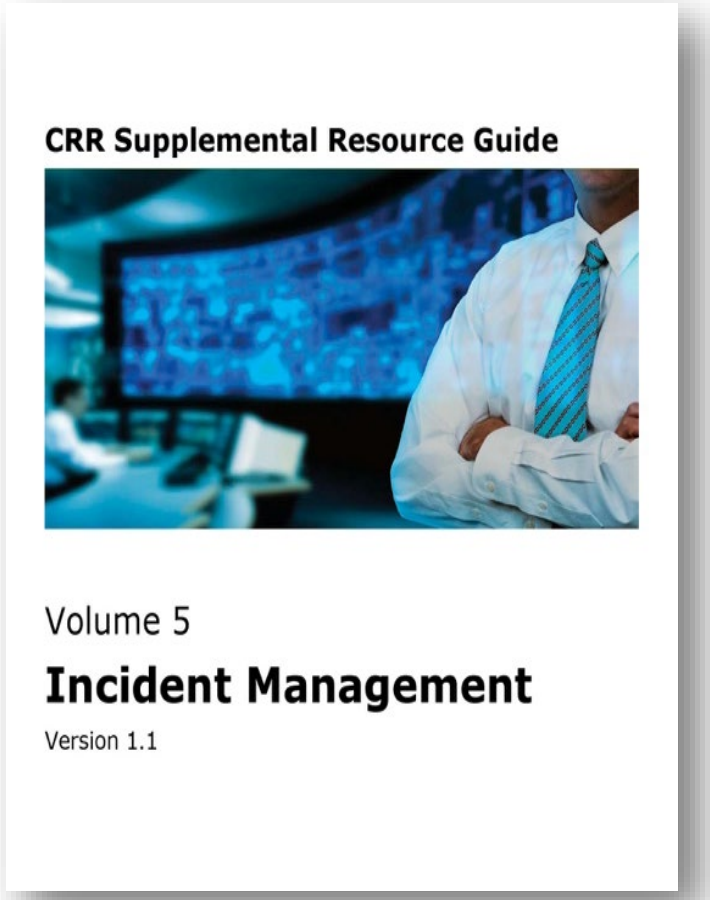
Key Resources

1. Criminal Justice Information Services (CJIS) Security Policy
2. NIST SP 800-61, Computer Security Incident Handling Guide
3. NIST SP 800-83, Guide to Malware Incident Prevention and Handling
4. NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response
5. California Emergency Support Function 18 Cybersecurity, Annex to the California State Emergency Plan
6. California Joint Cyber Incident Response Guide
7. Cybersecurity Incident & Vulnerability Response Playbooks, November 2021, Cybersecurity and Infrastructure Security Agency
8. CISA Stop Ransomware Guide

Incident Management Planning Helps Mitigate Effects

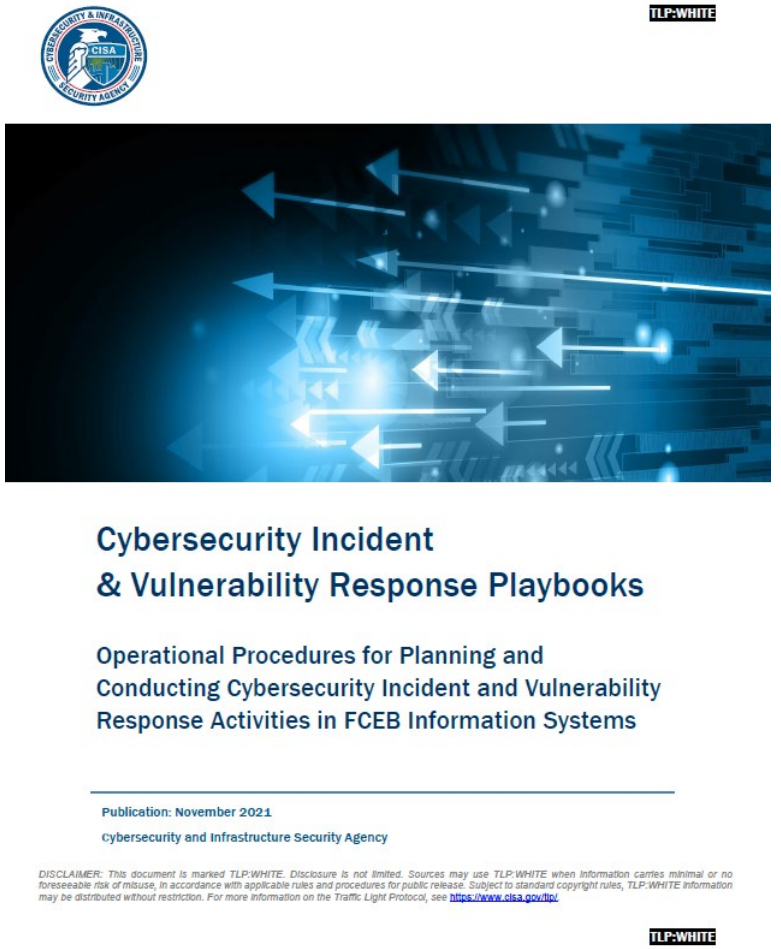
1. Get leadership support for incident management planning.
2. Establish an event-detection process.
3. Establish a triage-and-analysis process.
4. Establish an incident-declaration process.
5. Establish an incident-response and recovery process.
6. Establish an incident-communications process.
7. Assign roles and responsibilities for incident management.
8. Establish a post-incident analysis and improvement process.

Resource: CRR Supplemental Resource Guide, Incident Management.



Playbooks

- CISA tasked to develop a standard set of operational procedures (playbook) to be used in planning and conducting cybersecurity vulnerability and incident response activity respecting Federal Civilian Executive Branch (FCEB) Information Systems.
- Can be used by SLTT with little modification.
- Can be used at as a starting point.


TLP:WHITE

Cybersecurity Incident
& Vulnerability Response Playbooks

Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems

Publication: November 2021

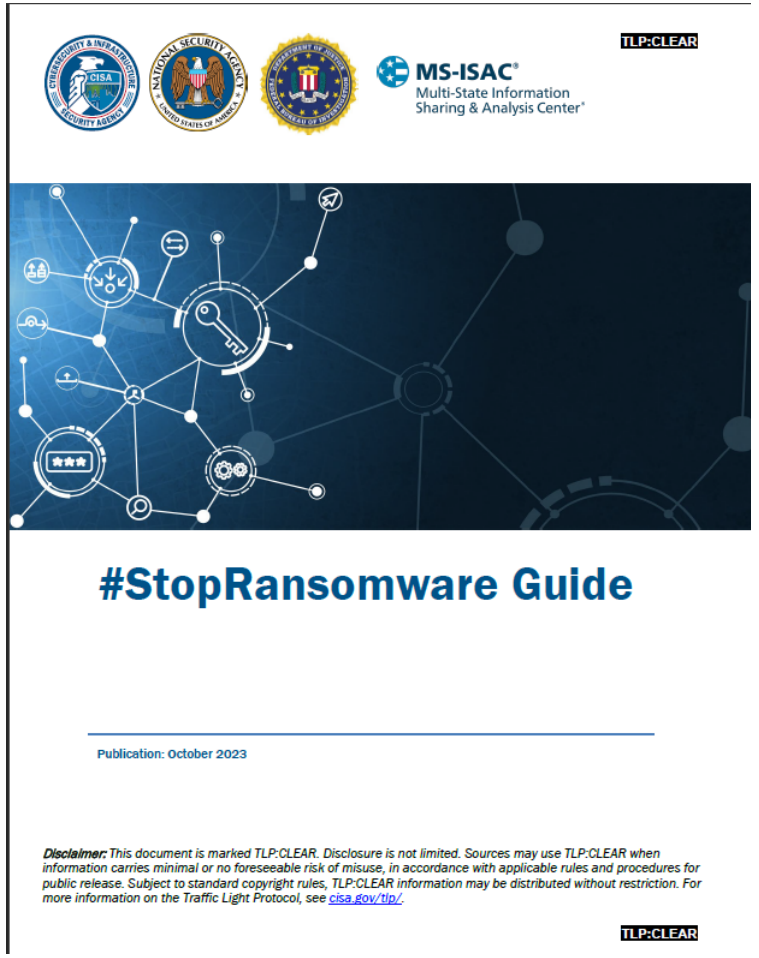
Cybersecurity and Infrastructure Security Agency

DISCLAIMER: This document is marked 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. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see https://www.cisa.gov/tlp/

TLP:WHITE

Ransomware Incident Response

- Guidance for preparation and response for ransomware
- This guide was developed through the U.S. Joint Ransomware Task Force (JRTF)
- Part 1: Ransomware and Data Extortion Prevention Best Practices
- Part 2: Ransomware and Data Extortion Response Checklist

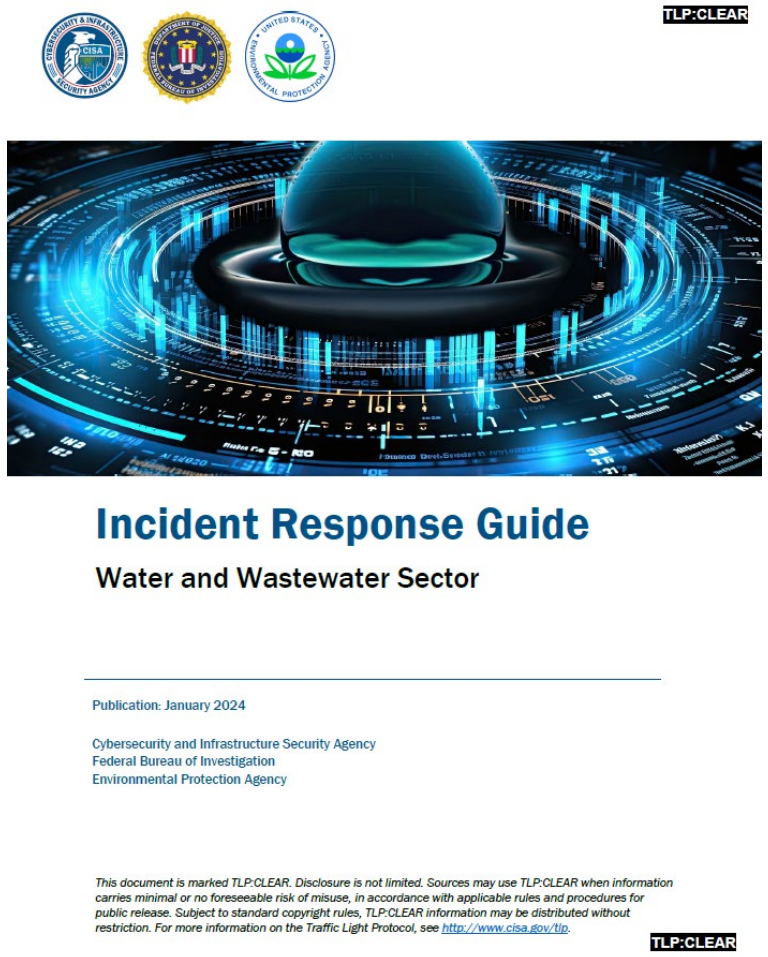


Latest update October 2023

CISA Technical Analysis and Support

- Tailored Guidance
- Technical Analysis*
  - Host Forensics
  - Network Forensics
  - Cloud Forensics
  - Cyber Physical Forensics (CPFS)
  - Automated Malware Analysis
  - Code and Media Analysis

* On a case-by-case basis, federal agencies may be able to provide no-cost tools and services to impacted utilities.


TLP:CLEAR

Incident Response Guide

Water and Wastewater Sector

Publication: January 2024

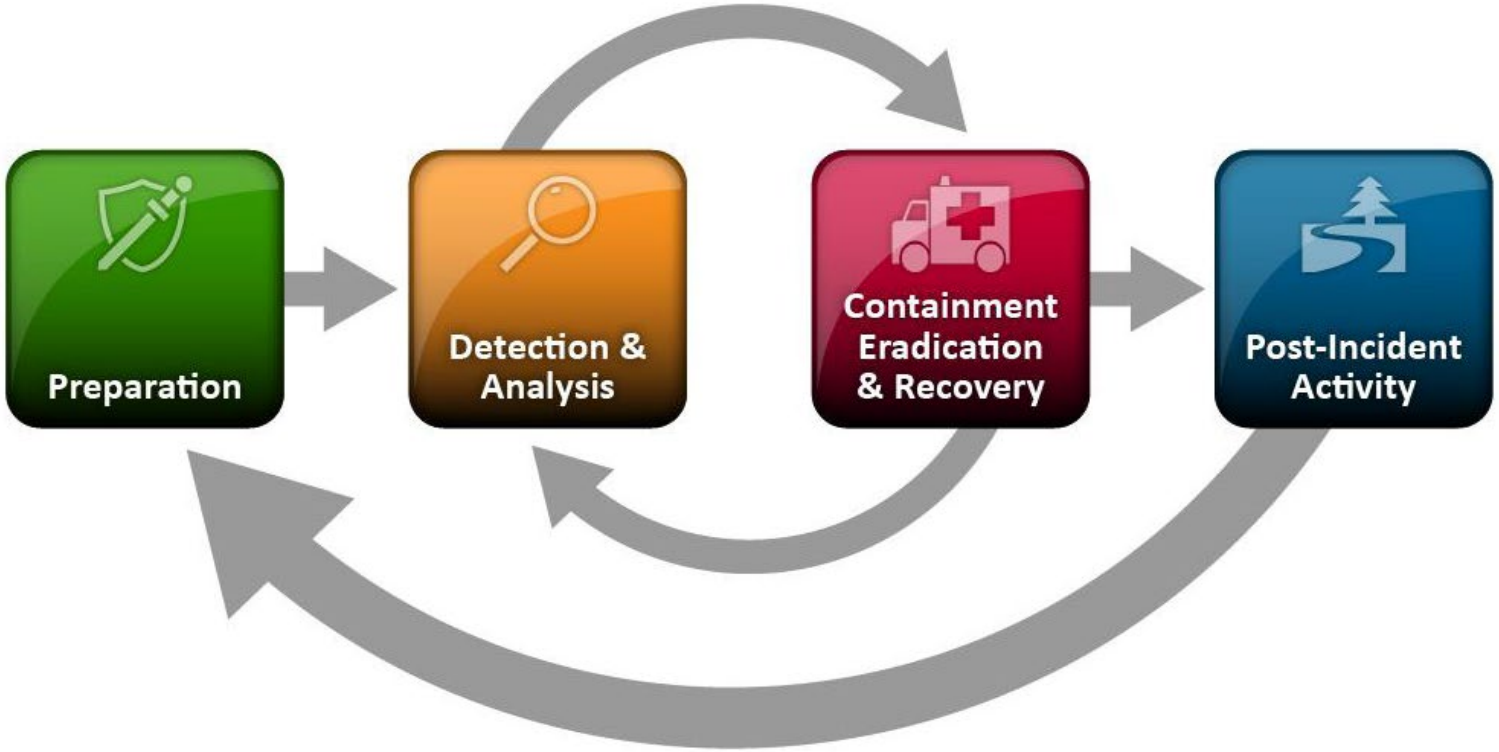
Cybersecurity and Infrastructure Security Agency
Federal Bureau of Investigation
Environmental Protection Agency

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR 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:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.cisa.gov/tlp.

TLP:CLEAR

Incident Response Guide, Water and Wastewater Sector, JAN 2024

Incident Response Life Cycle



Source: NIST SP 800-61 Revision 2, Computer Security Incident Handling Guide

Ransomware Incident Response

Detection and Analysis

Should your organization be a **victim of ransomware**, follow your approved Incident Response Plan (IRP) and associated run books.

We strongly recommend responding by using the following checklist. Be sure to move through the **first three steps in sequence**.

1. Determine which systems were impacted, and immediately **isolate them**.
2. Power down devices if you are unable to **disconnect them** from the network to avoid further spread of the ransomware infection. Only power down if you can't disconnect them.
3. Triage impacted systems for restoration and recovery.

Detection and Analysis (cont)

- Examine existing organizational detection or prevention systems (e.g., antivirus, EDR, IDS, Intrusion Prevention System) and logs.
- Confer with your team to develop and document an initial understanding of what has occurred based on initial analysis.
- Initiate threat hunting activities.

Cyber Incident Response Plan

Response Contacts:		
Contact	24x7 Contact Information	Roles and Responsibilities
IT/IT Security Team – Centralized Cyber Incident Reporting		
Departmental or Elected Leaders		
State and Local Law Enforcement		
Fusion Center		
Managed/Security Service Providers		
Cyber Insurance		

Reporting and Notification

- Follow notification requirements as outlined in your cyber incident response and communications plan to **engage internal and external teams and stakeholders** with an understanding of what they can provide to help you mitigate, respond to, and recover from the incident.
- If the incident resulted in a data breach, follow notification requirements as outlined in your cyber incident response and communications plans.
  - **Cyber Insurance Carrier (Legal council and incident responders)**
  - State and Federal Agencies
  - External Stakeholders (service providers, third parties, dependent parties, etc.)
  - Compliance Reporting (some may be time sensitive i.e. Payment Card Industry (PCI) or California Attorney General's office reporting)

Third Parties

- What about third parties you rely on?
- Do you have breach notification clause in your contact?
- When will they report an incident to you?
- Will it have an impact on services you deliver?
- What steps will you take to verify your systems are not impacted?

Containment and Eradication

- Take a system image and memory capture of a sample of affected devices (e.g., workstations, servers, virtual servers, and cloud servers).
- Consult federal law enforcement, even if mitigation actions are possible, regarding possible decryptors available.
- Research trusted guidance (e.g., published by sources such as the U.S. Government, MS-ISAC, or a reputable security vendor) for the particular ransomware variant and follow any additional recommended steps to identify and contain systems or networks that are confirmed to be impacted.
- Identify the systems and accounts involved in the initial breach.

Containment and Eradication (cont)

- Based on the breach or compromise details determined, contain associated systems that may be used for further or continued unauthorized access.
- If server-side data is being encrypted by an infected workstation, follow server-side data encryption quick identification steps.
- Conduct extended analysis to identify outside-in and inside-out persistence mechanisms.
- Rebuild systems based on prioritization of critical services.

Containment and Eradication (cont)

- Issue password resets for all affected systems and address any associated vulnerabilities and gaps in security or visibility.
- The designated IT or IT security authority declares the ransomware incident over based on established criteria.

Recovery and Post-Incident Activity

- Reconnect systems and restore data from offline, encrypted backups based on a prioritization of critical services.
  - Identify when first compromised and pull backups from prior to the infection date.
- Document lessons learned from the incident and associated response activities to inform updates to—and refine—organizational policies, plans, and procedures and guide future exercises of the same.
- Consider sharing lessons learned and relevant indicators of compromise with CISA or your sector ISAC to benefit others within the community.

WHO WE ARE

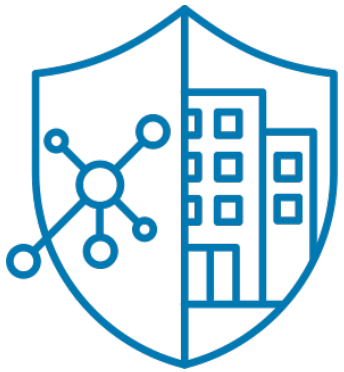
CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Who We Are

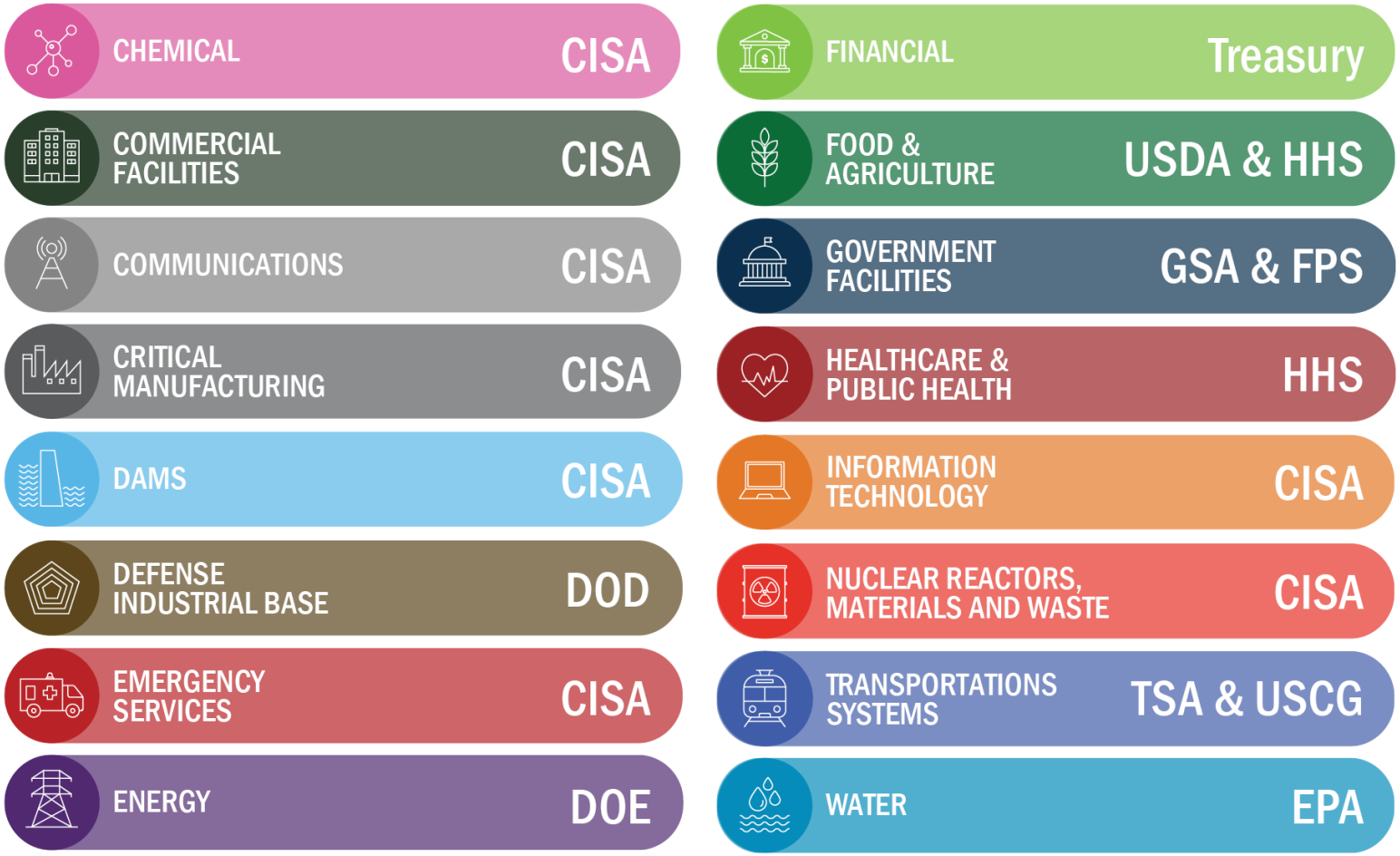
The Cybersecurity and Infrastructure Security Agency (CISA) is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future

CISA Mission and Vision

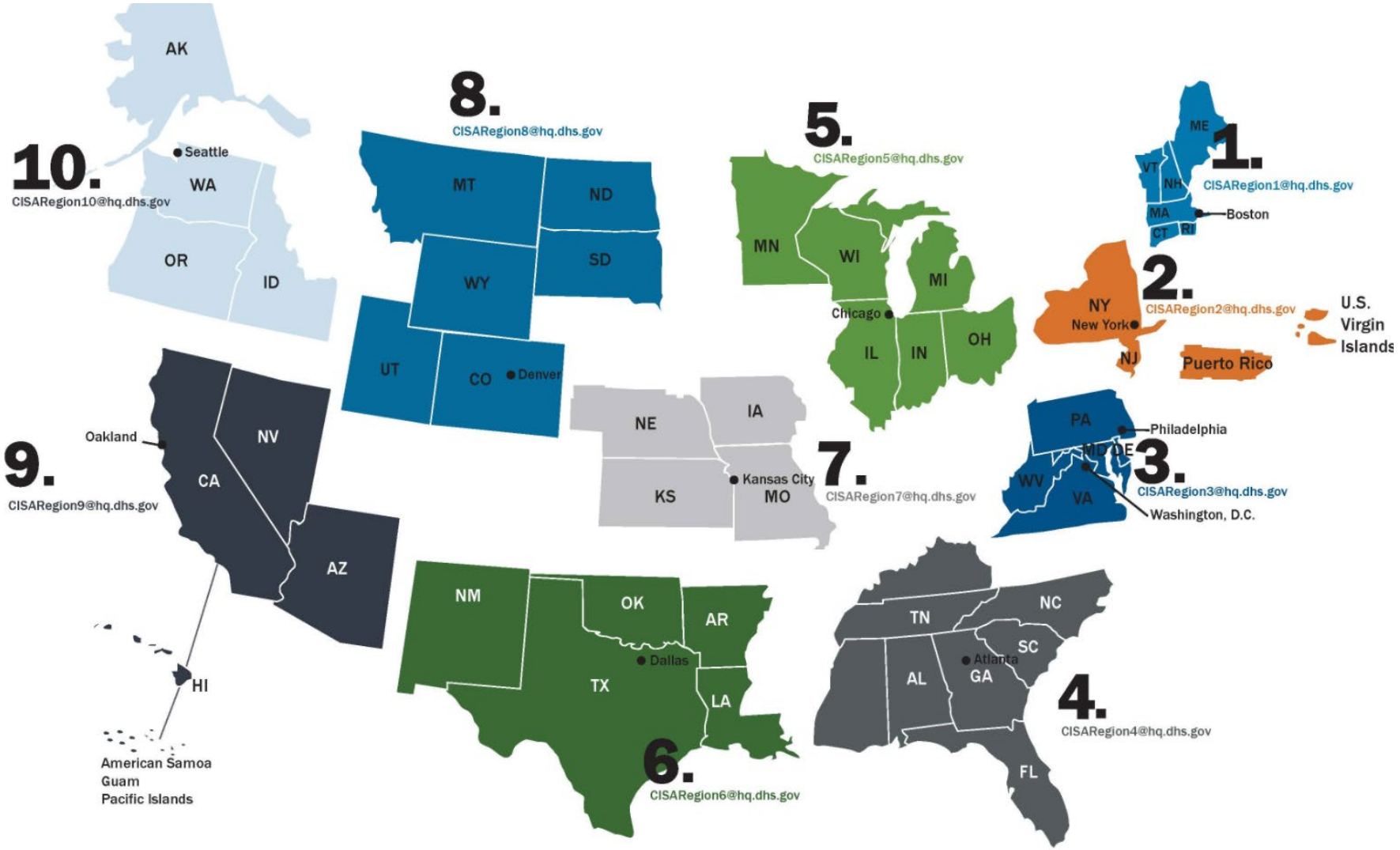
- Cybersecurity and Infrastructure Security Agency (CISA) mission:
  - Lead the collaborative national effort to strengthen the security and resilience of America's critical infrastructure
- CISA vision:
  - A Nation with secure, resilient, and reliable critical infrastructure upon which the American way of life can thrive



16 Critical Infrastructure Sectors & Corresponding Sector Risk Management Agencies



CISA Regions

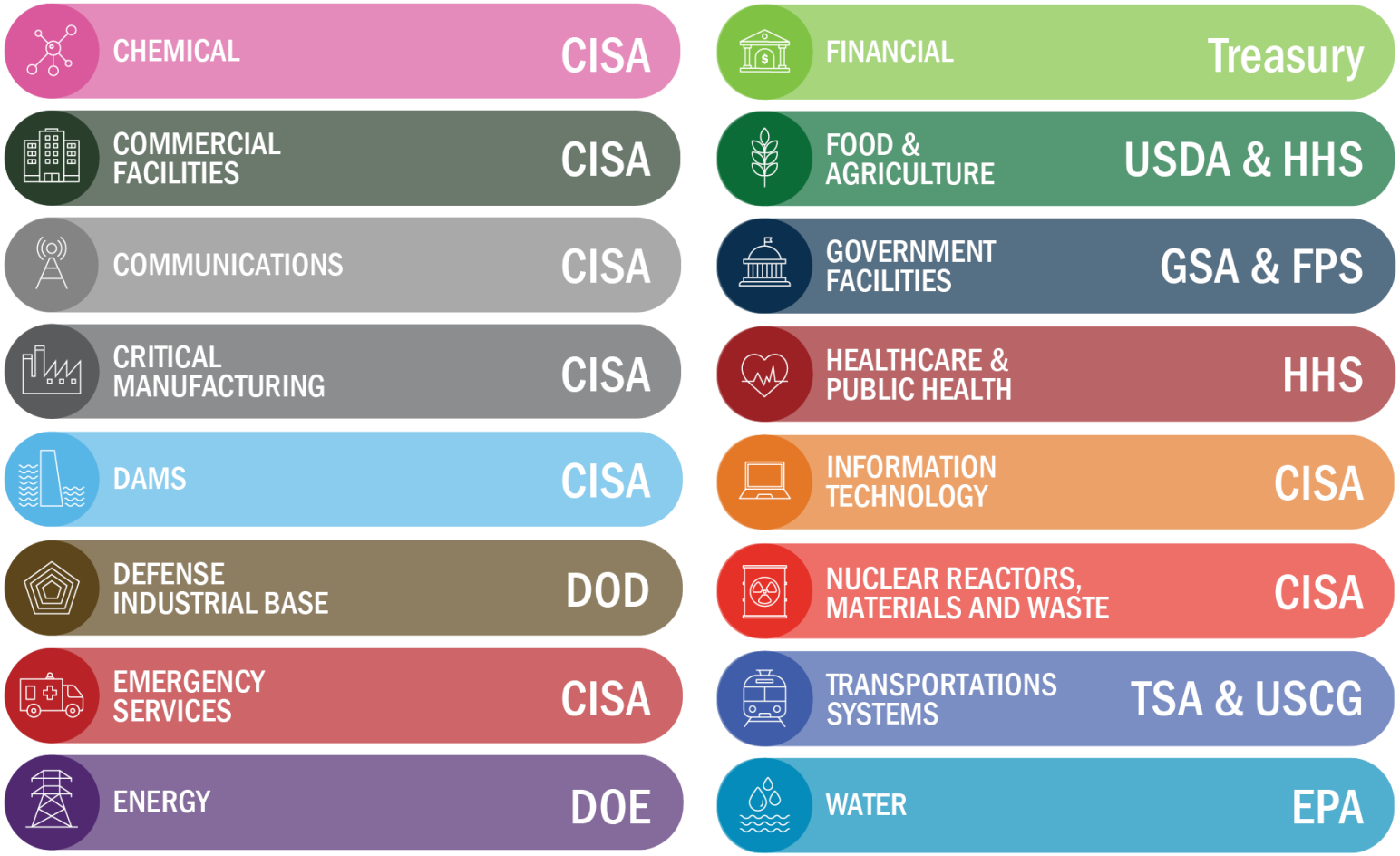


Regional Support

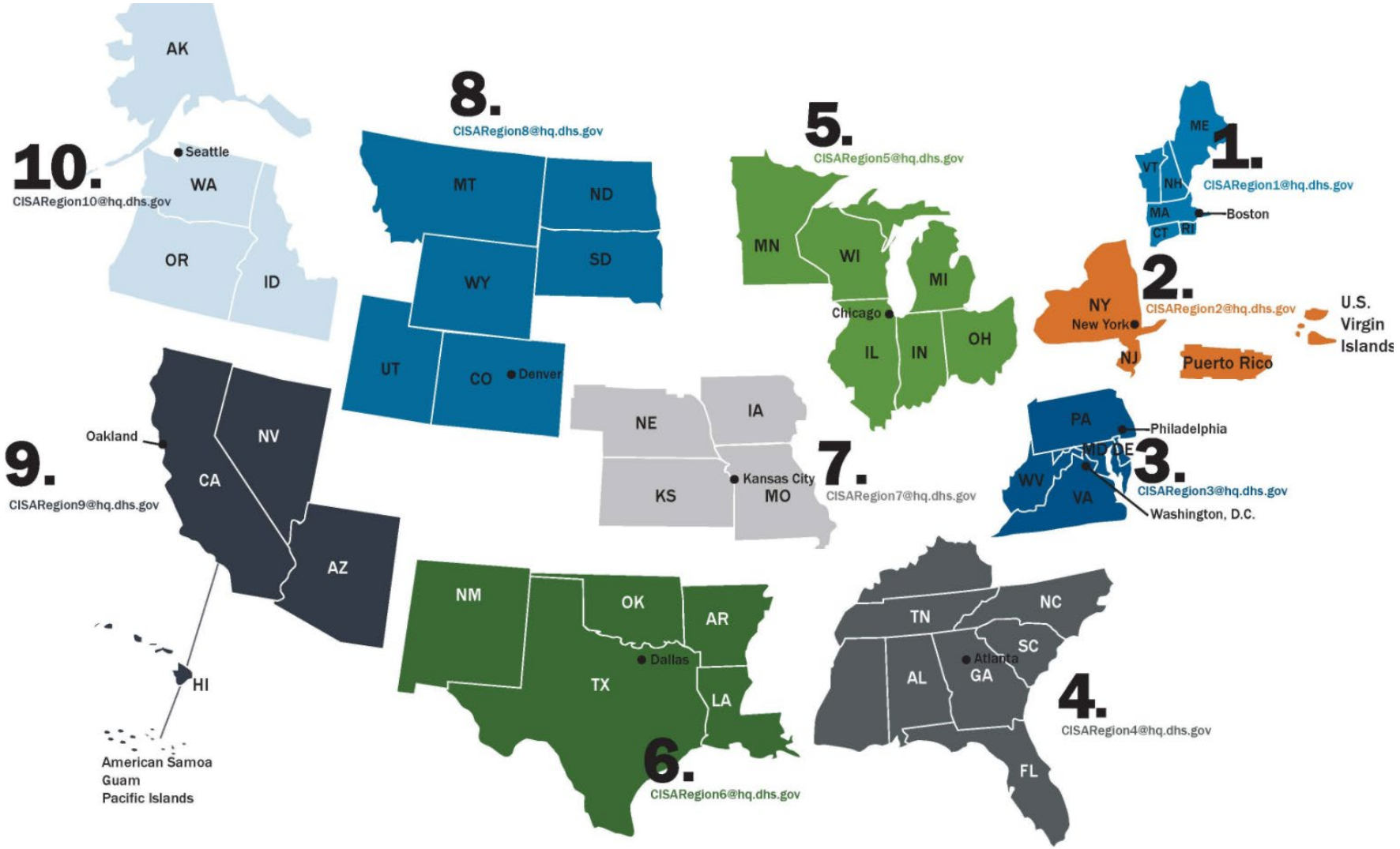
- Cybersecurity Advisors
- Protective Security Advisors
- Training and Exercise Specialists
- Chemical Security Advisors
- Election Security Advisors
- Emergency Communications Advisors

Region IX, All Hands Meeting (SEP 2023)

16 Critical Infrastructure Sectors & Corresponding Sector Risk Management Agencies



CISA Regions



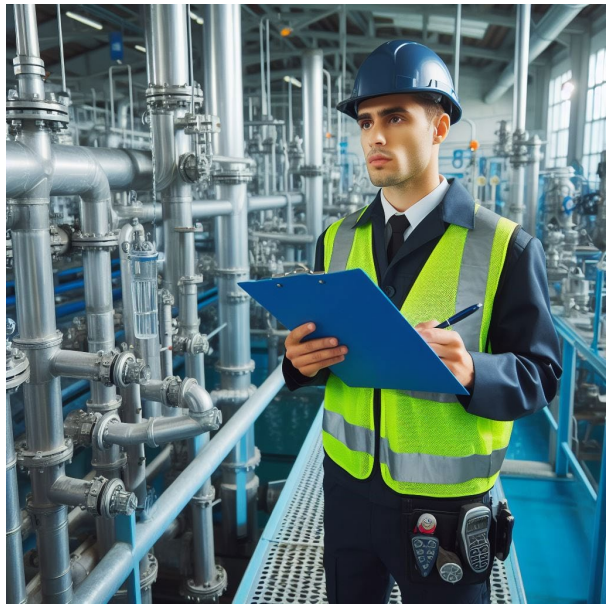
Regional Support

- Cybersecurity Advisors
- Protective Security Advisors
- Training and Exercise Specialists
- Chemical Security Advisors
- Election Security Advisors
- Emergency Communications Advisors

Region IX, All Hands Meeting (SEP 2023)

Protective Security Advisors

- Protective Security Advisors (PSA) are field-deployed personnel who serve as critical infrastructure security specialists
- State, local, tribal, territorial (SLTT) and private sector link to DHS infrastructure protection resources
  - Coordinate vulnerability assessments, training, and other DHS products and services
  - Provide a vital link for information sharing in steady state and incident response
  - Assist facility owners and operators with obtaining security clearances



Protective Security Advisors

SURVEYS AND ASSESSMENTS
PSAs conduct voluntary, non-regulatory security surveys and assessments on critical infrastructure assets and facilities within their respective regions.

OUTREACH ACTIVITIES
PSAs conduct outreach activities with critical infrastructure owners and operators, community groups, and faith-based organizations in support of CISA priorities.

SPECIAL EVENT SUPPORT
PSAs support Federal, State, and local officials responsible for planning, leading, and coordinating NSSE and SEAR events.

INCIDENT RESPONSE
PSAs plan for and, when directed, deploy in response to natural or man-made incidents.

BOMBING PREVENTION AND AWARENESS
PSAs work in conjunction with CISA's Office for Bombing Prevention by coordinating training and materials for partners to assist in deterring, detecting, preventing, protecting against, and responding to improvised explosive device threats.

Edgar S. Castor, CPP
Protective Security Advisor
Region 9: San Francisco District
Phone/Text: (202) 309-0715
Email: edgar.castor@hq.dhs.gov

Justin L. Brooks
Protective Security Advisor
Region 9: San Jose District
Phone/Text: (202) 819-6511
Email: justin.brooks@hq.dhs.gov

Christopher Reidel
Protective Security Advisor
Region 9: Sacramento District
Phone/Text: (207) 400-2769
Email: christopher.reidel@cisa.dhs.gov

Election Security Advisors

CISA Establishes Regional Election Security Advisors to Strengthen Front Line Support to the Election Community

- Support the election community
- Dedicated election security advisor
- Collaborate between state and local election officials
- Advisors for:
  - infrastructure,
  - jurisdictional requirements, and
  - operating environments

Susan Lapsley
Election Security Advisor
Region 9: AZ, CA, HI, NV, AS, CNMI, and GU
Phone/Text: (202) 550-3540
Email: Susan.Lapsley@cisa.dhs.gov

Training and Exercise

- Enables the cyber-ready workforce of tomorrow by leading training and education for the cybersecurity workforce.
- Conducts cyber and physical security exercises & training with government and industry partners to enhance security and resilience of critical infrastructure.

Ashley M. Lerner
Regional Training and Exercise Coordinator
Region 9: AZ, CA, HI, NV, AS, CNMI, and GU
Phone/Text: (202) 704-9373
Email: ashley.lerner@cisa.dhs.gov

CISA Cybersecurity Advisors (California)

Southern California
Supervisory CSA Pending
first.last@cisa.dhs.gov
(202) ###-####

Los Angeles CSA
CSA Pending
first.last@cisa.dhs.gov
202-###-####

Orange County CSA
CSA Jacob Aguiar
jacob.aguiar@cisa.dhs.gov
202-957-3040

Riverside CSA
CSA Aaron Dombrowski
aaron.dombrowski@cisa.dhs.gov
202-805-6785

San Diego CSA
CSA Vincent Chapman
Vincent.chapman@cisa.dhs.gov
(202) 285-2346

Region 9 Chief of Cyber
CCY Joseph Oregón
joseph.oregon@hq.dhs.gov
(202) 669-1817

Northern California & Pacific
Supervisory CSA Mario Garcia
mario.garcia@cisa.dhs.gov
(202) 309-1847

California CSC (Sacramento)
CSC Pending
first.last@cisa.dhs.gov
(202) ###-####

San Francisco CSA
CSA Donald Hester
donald.hester@cisa.dhs.gov
(202) 315-8091

San Jose CSA
CSA Scott Alford
scott.alford@cisa.dhs.gov
(202) 285-9621

Fresno CSA
CSA Timothy Villareal
timothy.villareal@cisa.dhs.gov
(202) 294-3395

Rev. 2/6/2024

Other Contacts

Reporting

- In responding to any cyber incident, Federal agencies may undertake threat response; asset response; and intelligence support and related activities.
- CISA: To report anomalous cyber activity and/or cyber incidents 24/7, email **report@cisa.gov**, or call **(888) 282-0870**.
- MS-ISAC: For SLTTs, email **soc@msisac.org** or call **(866) 787-4722**

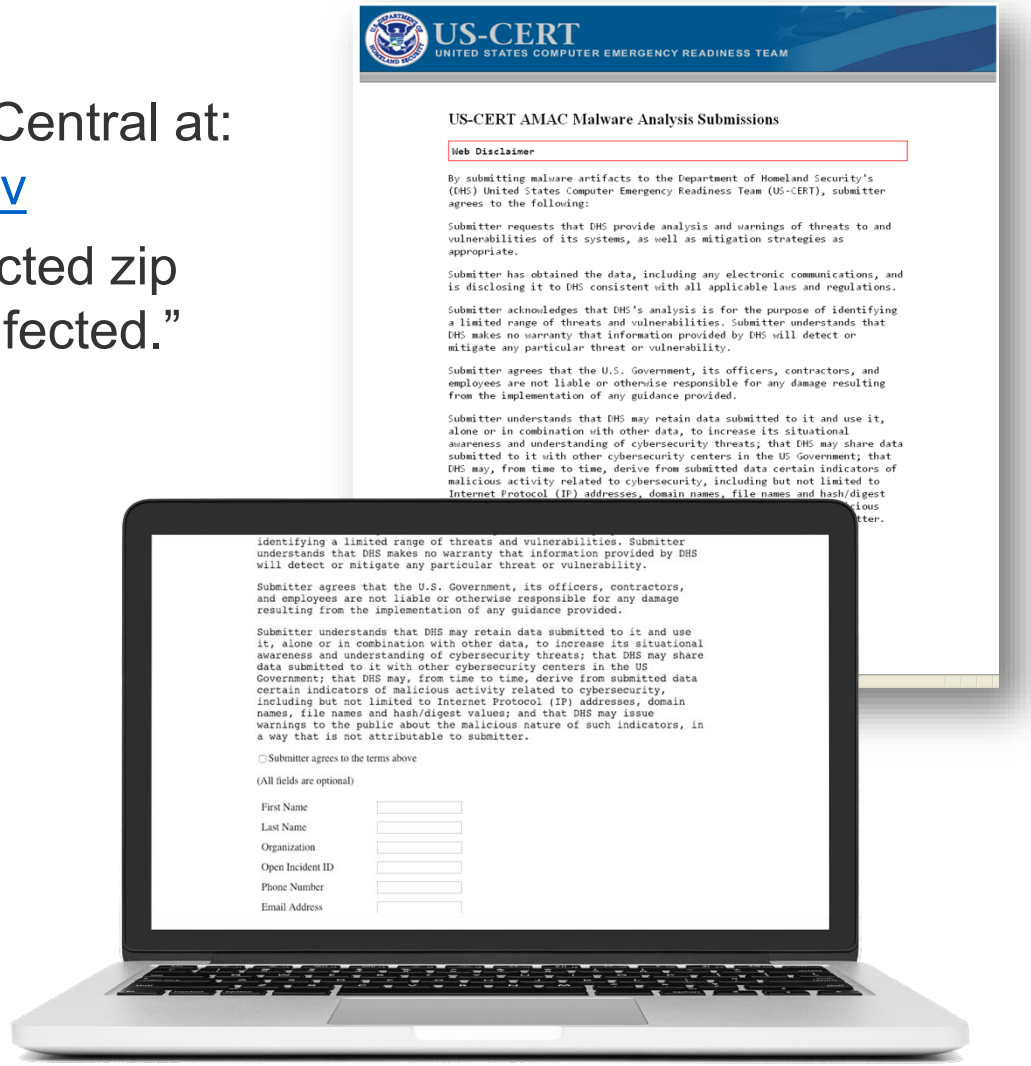
Upon voluntary request, CISA and MS-ISAC (for SLTT organizations) can assist with analysis of phishing emails, storage media, logs, and/or malware at no cost to help organizations understand the root cause of an incident.

- CISA – Advanced Malware Analysis Center: malware.us-cert.gov/
- MS-ISAC – Malicious Code Analysis Platform (SLTT organizations only): cisecurity.org/spotlight/cybersecurity-spotlight-malware-analysis/

Malware Analysis

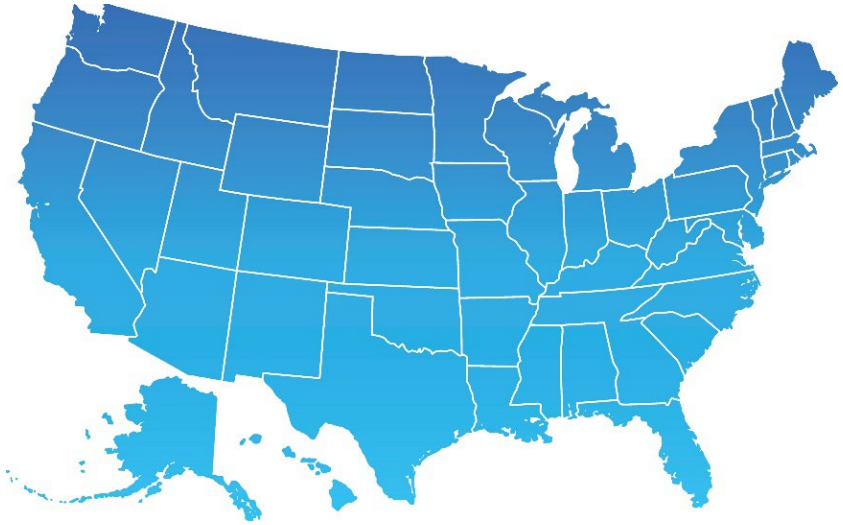
To submit malware:

- Email submissions to CISA Central at: submit@malware.us-cert.gov
  - Send in password-protected zip file(s). Use password “infected.”
- Upload submission online: https://malware.us-cert.gov



Information Sharing Opportunities

- Multi-State Information Sharing and Analysis Center
  - Focal point for cyber threat prevention, protection, response and recovery for state, local, tribal, and territorial governments.
  - Operates 24 x7 cyber security operations center, providing real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification and mitigation and incident response. For more information, visit www.cisecurity.org/ms-isac or email info@msisac.org



- ISACs and ISAOs
  - **Information Sharing and Analysis Centers** (ISACs) or **Organizations** (ISAOs) are communities of interest sharing cybersecurity risk, threat information, and incident management to members. For more information on ISACs, visit www.nationalisacs.org. For more on ISAOs visit www.isao.org/about.

MS-ISAC

- Multi-State Information Sharing and Analysis Center
- As a trusted cybersecurity partner for 13,000+ U.S. State, Local, Tribal, and Territorial (SLTT) government organizations.
- Cultivate a collaborative environment for information sharing in support of our mission.
- Offer members incident response and remediation support and develop tactical, strategic, and operational intelligence, and advisories that offer actionable information for improving cyber maturity.

California Fusion Centers

The California Fusion Centers serve as California's information sharing clearinghouse of strategic threat analysis and situational awareness reporting to statewide leadership and the public safety community in support of efforts to prevent, prepare for, mitigate and respond to all crimes and all hazards impacting California citizens and critical infrastructure, while preserving civil liberties, individual privacy, and constitutional rights.

Regional Contacts

- Central California Intelligence Center (CCIC)
  - Sacramento | sacrtac.org | **(888) 884-8383**
- Northern California Regional Intelligence Center (NCRIC)
  - San Francisco | ncric.ca.gov | **(866) 367-8847**
- The Joint Regional Intelligence Center (JRIC)
  - Los Angeles | jric.org | **(563) 345-1100**
- Orange County Intelligence Assessment Center (OCIAC)
  - Santa Ana | ociac.ca.gov | **(714) 289-3949**
- San Diego Law Enforcement Coordination Center (SD-LECC)
  - San Diego | sdlecc.org | **(858) 495-7200**

Cal-CSIC

- The California Cybersecurity Integration Center's (Cal-CSIC) mission is to reduce the number of cyber threats and attacks in California.
- The Cal-CSIC's focus is to **respond to cyber threats and attacks** that could damage the economy, its critical infrastructure, or computer networks in the state.
- Report cyber incidents to the Cal-CSIC at **(833) REPORT-1** or **calcsic@caloes.ca.gov**.

FBI Field Offices

Los Angeles
11000 Wilshire Boulevard, Suite 1700
Los Angeles, CA 90024
losangeles.fbi.gov
(310) 477-6565

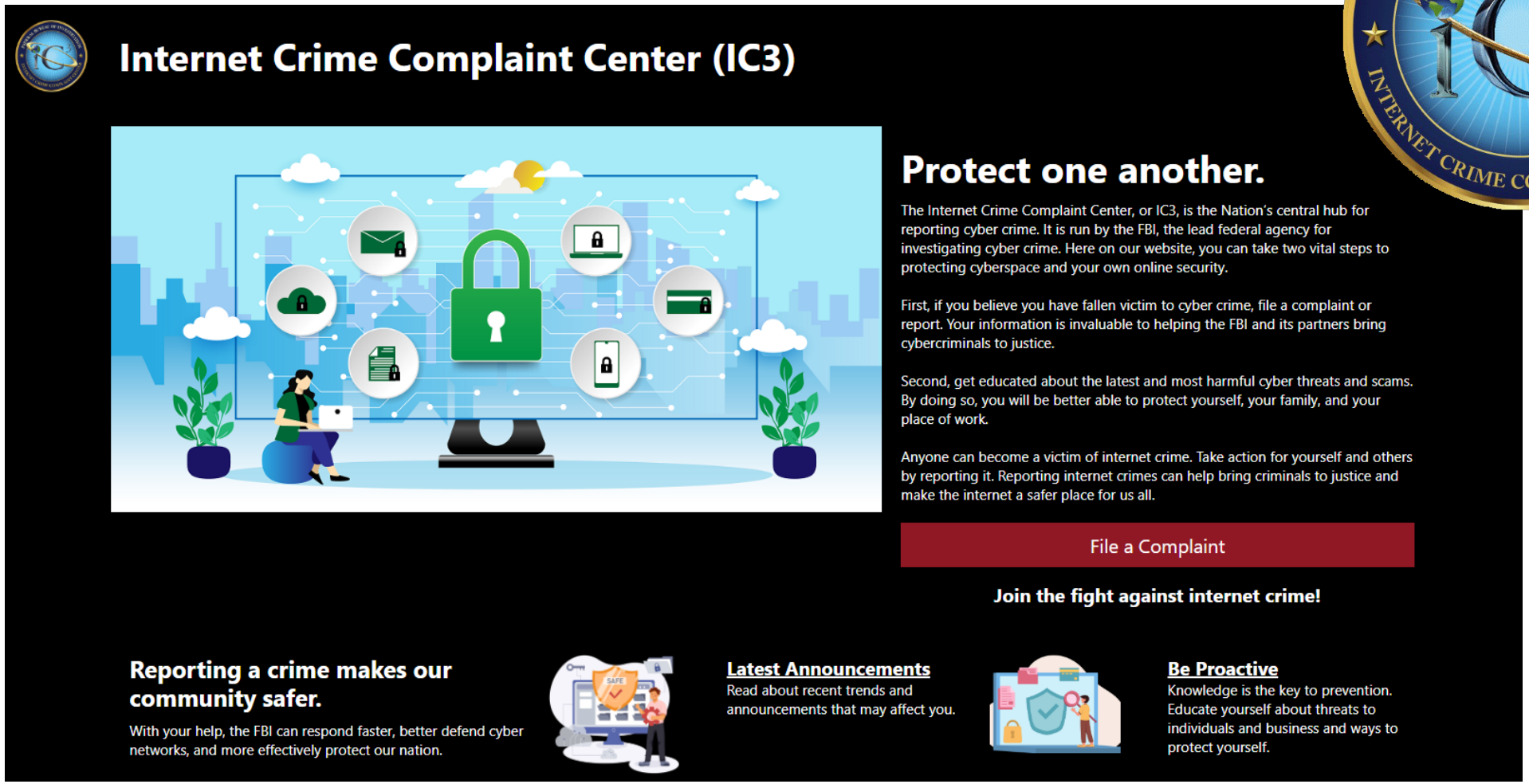
Sacramento
2001 Freedom Way
Roseville, CA 95678
sacramento.fbi.gov
(916) 746-7000

San Francisco
450 Golden Gate Avenue, 13th Floor
San Francisco, CA 94102-9523
sanfrancisco.fbi.gov
(415) 553-7400

San Diego
10385 Vista Sorrento Parkway
San Diego, CA 92121
sandiego.fbi.gov
(858) 320-1800

https://www.fbi.gov/contact-us/field-offices

IC3.gov



https://www.ic3.gov/

United States Secret Service

- Cyber Fraud Task Forces (CFTFs), investigate cyber crimes involving financial fraud.
- The strategically located CFTFs combat cybercrime through prevention, detection, mitigation, and investigation.
- Los Angeles | **(213) 894-4830**
- San Diego | **(619) 557-5640**
- San Francisco | **(415) 576-1210**

Who do you call?

- Internal Contacts (Out-of-band)
- Insurance Provider
- Service Providers (Especially cloud service providers, MSSPs, key vendors)
- Incident Responders (Do you have them on retainer?)

CISA Resources

Resource Guides

- **Resource Guides:** Created to help organizations enhance their resilience in specific Cyber Resilience Review (CRR) domains.
- **CRR Tools:** Helps move organizations from initial capability to well-define capability in security management areas
- **CRR Domains**: Includes the CRR 10 “domains” each representing a capability area foundational to an organization’s cyber resilience.
- **Content**: While the guides were developed for organizations to utilize after conducting a CRR, these publications provide content useful for all organizations with cybersecurity equities.
- **Flexibility in Use**: Moreover, the guides can be utilized as a full set or as individual components, depending on organizational preference and/or need.
- For more information, visit https://www.cisa.gov/cyber-resource-hub

Cybersecurity Services

- Cybersecurity Advisors
- State, Local, Tribal, and Territorial engagements
- Cyber Education and Awareness
- Federal Virtual Training Environment (Fed VTE)
- National Initiative for Cybersecurity Careers and Studies (NICCS)
- Stop. Think. Connect.™
- Cybersecurity Awareness Month
- .gov Domain
- Request a CISA Speaker
- Biweekly Threat Briefing
- Information / Threat Indicator Sharing
- Known Exploited Vulnerabilities Catalog
- Resource Guides
- Cyber Incident Response Tabletop Exercise (TTX)
- Advanced Malware Analysis Center

- Cyber Performance Goals (CPG)
- Ransomware Readiness Assessment (RRA)
- Cyber Resilience Reviews (CRR™)
- External Dependencies Management (EDM) Assessments
- Cyber Infrastructure Survey
- Cyber Security Evaluation Tool (CSET™)
- Cyber Hygiene Services
  - Vulnerability Scanning
  - Web Application Scanning (WAS)
  - Ransomware Vulnerability Warning Pilot (RVWP)
- Risk and Vulnerability Assessment (RVA)
- Validated Architecture Design Review (VADR)
- Critical Infrastructure (CI) Shared Services Pilots
  - CyberSentry*
  - Protective DNS*
  - Secure Cloud Business Applications (SCuBA)*
  - Logging Made Easy (LME)*

Range of Cybersecurity Assessments

- Cyber Resilience Review (Strategic)
- External Dependencies Management (Strategic)
- Cyber Infrastructure Survey (Strategic)
- Cybersecurity Evaluations Tool (Strategic/Technical)
- Cyber Performance Goals (EVERYONE)
- Vulnerability Scanning / Hygiene (Technical)
- Validated Architecture Design Review (Technical)
- Risk and Vulnerability Assessment (Technical)

Cyber Performance Goals

- Voluntary self-assessment
- Baseline set of cybersecurity practices
- Broadly applicable across critical infrastructure
- Known risk-reduction value
- Recommended practices for IT and OT owners
- Guided self-assessment
- Not a full cybersecurity program

IDENTIFY (1)

1.A Asset Inventory — ID.AM-1, ID.AM-2, ID.AM-4, DE.CM-1, DE.CM-7	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: $$$$ IMPACT: HIGH COMPLEXITY: MEDIUM TACTIC, TECHNIQUE, AND PROCEDURE (TTP) OR RISK ADDRESSED: Hardware Additions (T1200) Exploit Public-Facing Application (T0819, ICS T0819) Internet-accessible device (ICS T0883) RECOMMENDED ACTION: Maintain a regularly updated inventory of all organizational assets with an IP address (including IPv6), including OT. This inventory is updated on a recurring basis, no less than monthly for both IT and OT. FREE SERVICES AND REFERENCES: Cyber Hygiene Services, "Stuff Off Search" Guide or email vulnerability@cisa.DHS.gov	DATE: IMPLEMENTED IN PROGRESS SCOPED NOT STARTED	DATE: IMPLEMENTED IN PROGRESS SCOPED NOT STARTED	

1.B Organizational Cybersecurity Leadership — ID.GV-1, ID.GV-2	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: $ IMPACT: HIGH COMPLEXITY: LOW TTP OR RISK ADDRESSED: Lack of sufficient cybersecurity accountability, investment, or effectiveness. RECOMMENDED ACTION: A named role/position/title is identified as responsible and accountable for planning, resourcing, and execution of cybersecurity activities. This role may undertake activities, such as managing cybersecurity operations at the senior level, requesting and securing budget resources, or leading strategy development to inform future positioning.	DATE: IMPLEMENTED IN PROGRESS SCOPED NOT STARTED	DATE: IMPLEMENTED IN PROGRESS SCOPED NOT STARTED	

1.C OT Cybersecurity Leadership — ID.GV-1, ID.GV-2	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: $ IMPACT: HIGH COMPLEXITY: LOW TTP OR RISK ADDRESSED: Lack of accountability, investment, or effectiveness of OT cybersecurity program. RECOMMENDED ACTION: A named role/position/title is identified as responsible and accountable for planning, resourcing, and execution of OT-specific cybersecurity activities. In some organizations this may be the same position as identified in 1.B.	DATE: IMPLEMENTED IN PROGRESS SCOPED NOT STARTED	DATE: IMPLEMENTED IN PROGRESS SCOPED NOT STARTED	

1.D Improving IT and OT Cybersecurity Relationships — ID.GV-2, PR.AT-5	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: $ IMPACT: MEDIUM COMPLEXITY: LOW TTP OR RISK ADDRESSED: Poor working relationships and a lack of mutual understanding between IT and OT cybersecurity can often result in increased risk for OT cybersecurity. RECOMMENDED ACTION: Organizations sponsor at least one "pizza party" or equivalent social gathering per year that is focused on strengthening working relationships between IT and OT security personnel, and is not a working event (such as providing meals during an incident response).	DATE: IMPLEMENTED IN PROGRESS SCOPED NOT STARTED	DATE: IMPLEMENTED IN PROGRESS SCOPED NOT STARTED	

Vulnerability Scanning

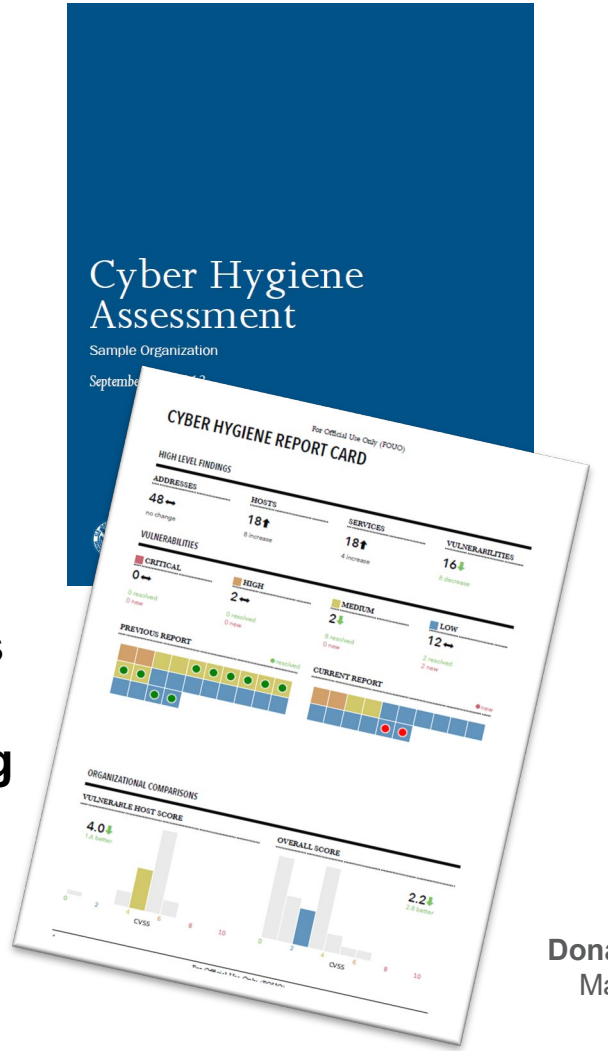
Purpose: Assess Internet-accessible systems for known vulnerabilities and configuration errors.

Delivery: Online by CISA

Benefits:

- Continual review of system to identify potential problems
- Weekly reports detailing current and previously mitigated vulnerabilities
- Recommended mitigation for identified vulnerabilities

  - **Network Vulnerability & Configuration Scanning**
    - Identify network vulnerabilities and weakness



Cybersecurity Awareness Month

The National Cybersecurity Alliance creates strong partnerships between governments and corporations to amplify our message and to foster a greater “digital” good.

Each and every one of us needs to do our part to make sure that our online lives are kept safe and secure. That’s what Cybersecurity Awareness Month is all about!

Established in 2001
2.1 Mil page views in 2021
30k Newsletter subscribers
360k Social media followers

Request a CISA Speaker

- CISA maximizes its resources through unified integrated and cohesive stakeholder activities by engaging in speaking events and conferences.
- Follow the steps at the “Request a CISA Speaker” page to request a CISA speaker for your Cybersecurity Awareness Month event.
- https://www.cisa.gov/news-events/request-speaker

City of Orinda Council Meeting

Checklist

- Attend CISA, MS-ISAC, & Cal-CSIC threat briefs
- Sign up for notifications from FBI, CISA, and Cal-CSIC Morning Report
- Contact your local Cybersecurity Advisor (CSA) & Protective Security Advisor (PSA)
- Sign up for Cyber Hygiene scanning service
- Contact CSA for guided self-assessment of the Cyber Performance Goals (CPG)
- Schedule a Tabletop Exercise
- Contact PSA for physical security assessment
- Find more at https://www.cisa.gov/resources-tools/services

Get .gov Domain

- Get .gov Domain. It should be easy to identify governments on the internet.
- The public shouldn’t have to guess whether the site they’re on or the email that hits their inbox is genuine.
- .gov is the top-level domain for U.S.-based government organizations.
- CISA sponsors the .gov TLD and makes it available solely to U.S.-based government organizations and publicly controlled entities.
- For those that qualify for a .gov domain, it’s available without a fee. For more information or to register go to https://get.gov/
- For questions email registrar@dotgov.gov


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY