CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

RANSOMWARE INCIDENT RESPONSE

Donald E. Hester
CISA Cybersecurity Advisor – San Francisco Bay Area
Cybersecurity Advisor Program
Cybersecurity and Infrastructure Security Agency

Cell: +1 (202) 315-8091
Teams: +1 (202) 984-3677
Email: donald.hester@cisa.dhs.gov

Fall 2023

WHO WE ARE

CISA Mission and Vision

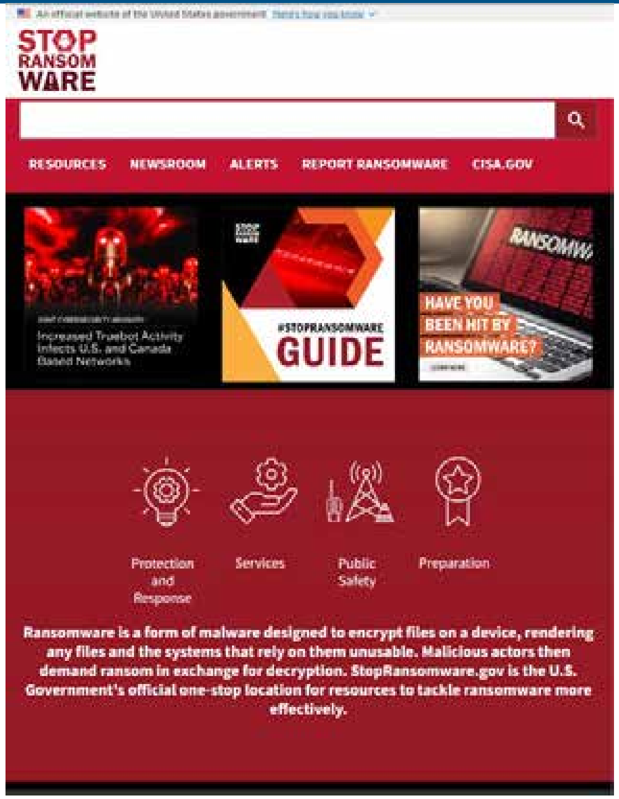
- Cybersecurity and Infrastructure Security Agency (CISA) mission:
  - Lead the collaborative national effort to strengthen the security and resilience of America’s critical infrastructure
- CISA vision:
  - A Nation with secure, resilient, and reliable critical infrastructure upon which the American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

Cybersecurity and Resilience

Who is targeting you?

What is Ransomware?

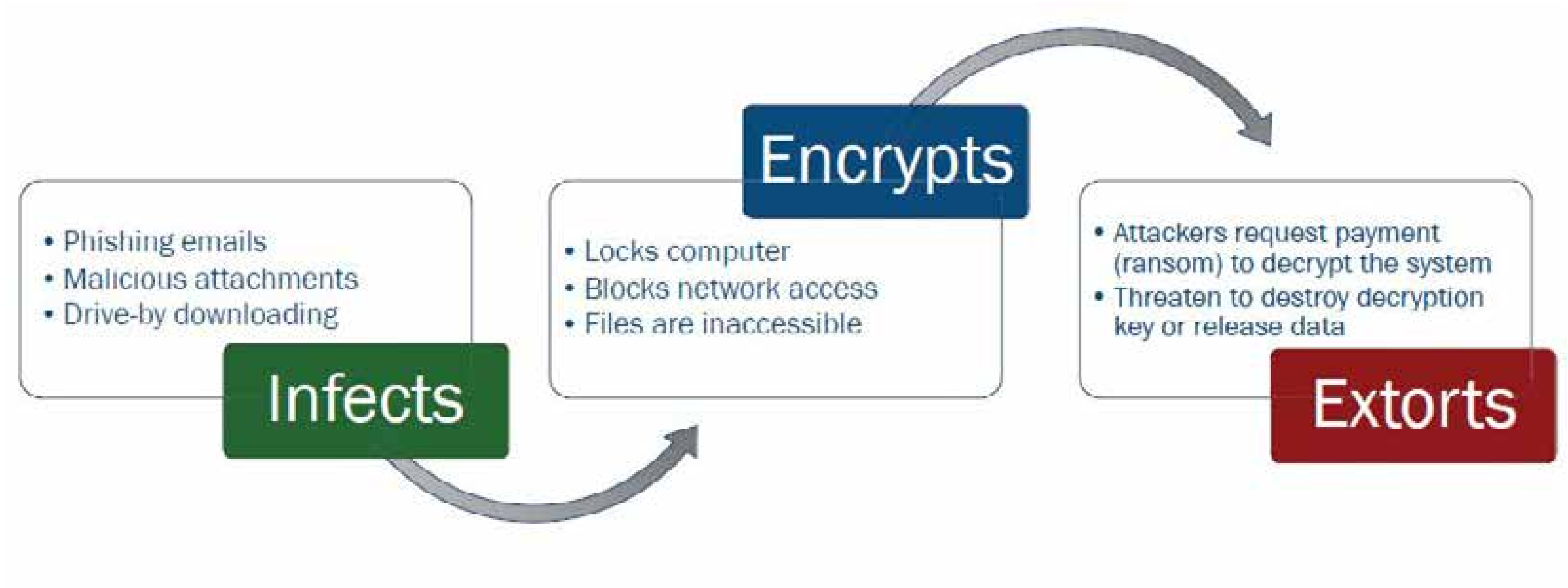
- Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable.
- Malicious actors then demand ransom in exchange for decryption.
- StopRansomware.gov is the U.S. Government's official one-stop location for resources to tackle ransomware more effectively.


An official website of the United States government Here's how you know
STOP RANSOM WARE
RESOURCES
NEWSROOM
ALERTS
REPORT RANSOMWARE
CISA.GOV
Increased Truebot Activity Infects U.S. and Canada Based Networks
#STOPRANSOMWARE GUIDE
RANSOMWA
HAVE YOU BEEN HIT BY RANSOMWARE?
Protection and Response
Services
Public Safety
Preparation

Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. StopRansomware.gov is the U.S. Government's official one-stop location for resources to tackle ransomware more effectively.

stopransomware.gov

Ransomware Patterns of Behavior



Infects

- Phishing emails
- Malicious attachments
- Drive-by downloading

Encrypts

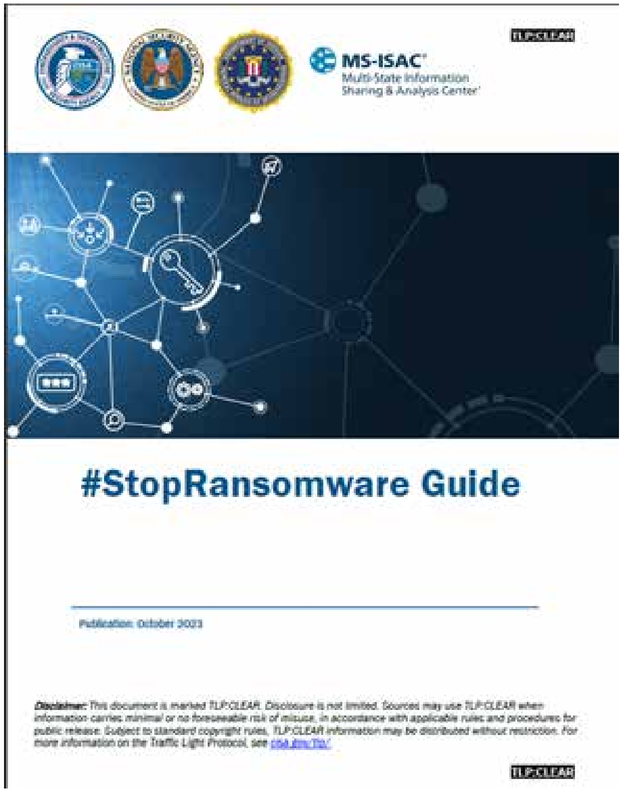
- Locks computer
- Blocks network access
- Files are inaccessible

Extorts

- Attackers request payment (ransom) to decrypt the system
- Threaten to destroy decryption key or release data

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



TLP:CLEAR

MS-ISAC
Multi-State Information
Sharing & Analysis Center

#StopRansomware Guide

Publication: October 2023

Disclaimer: *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* cisa.gov/tlp/.

TLP:CLEAR

Latest update October 2023

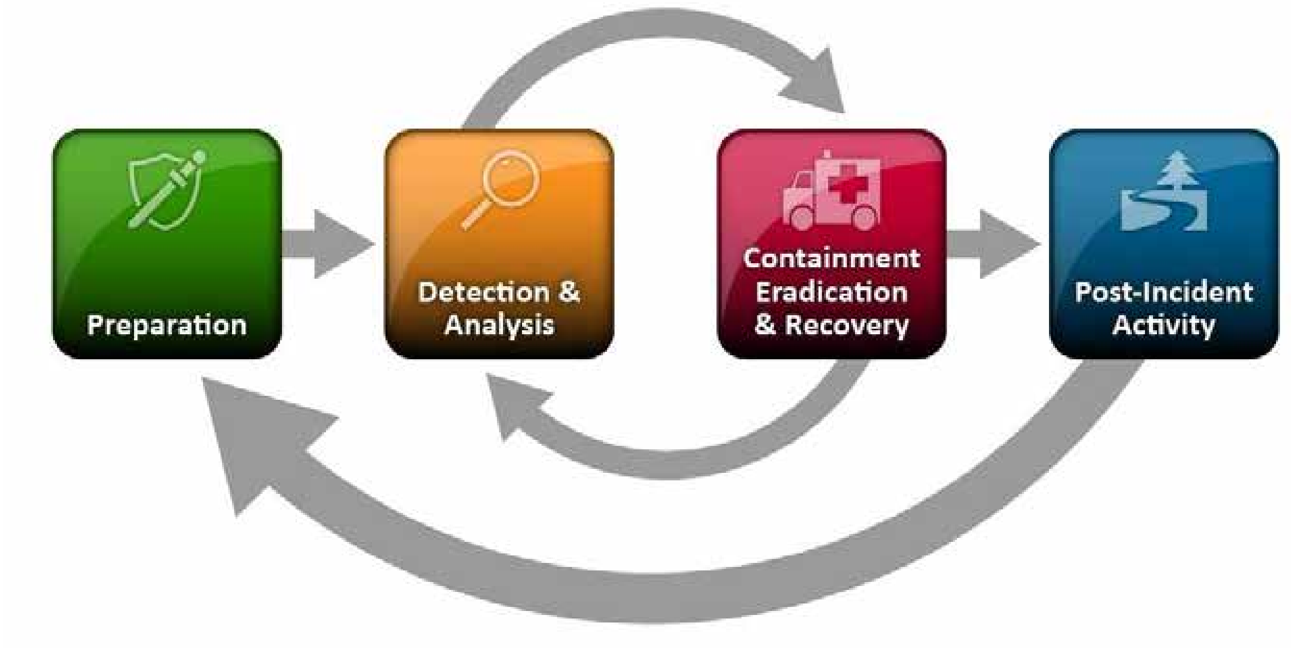
Detection and Analysis

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.

Incident Response Life Cycle



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

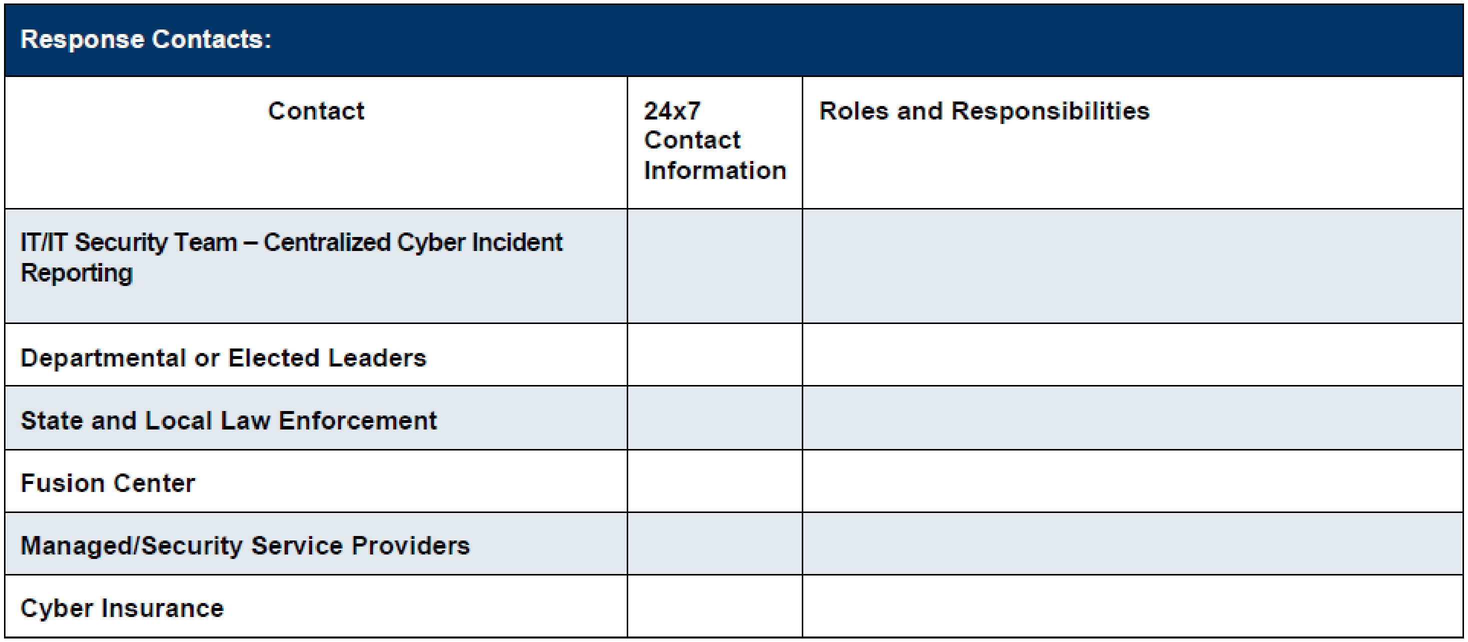
Detection and Analysis (cont)

- 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.

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
  - 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)

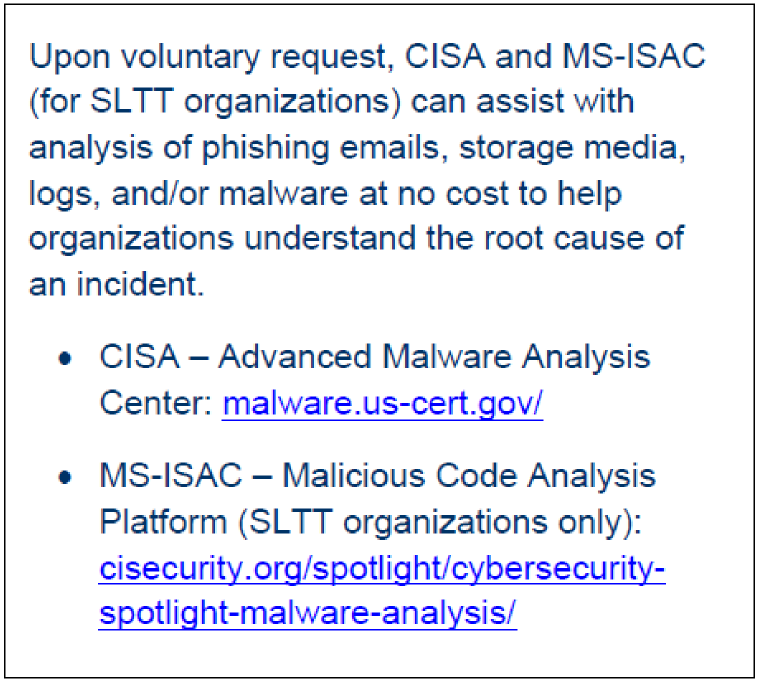
Cyber Incident Response Plan



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

- 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**



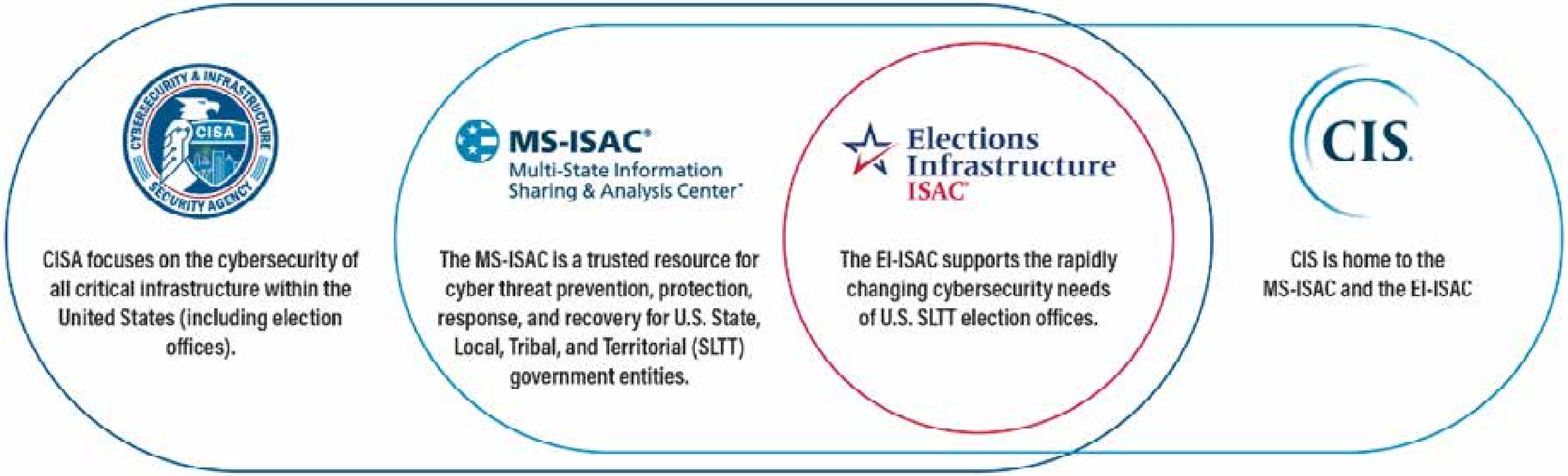
Upon voluntary request, CISA and MS-ISAC (for SLTT organizations) can assist with analysis of phishing emails, storage media, logs, and/or malware at no cost to help organizations understand the root cause of an incident.

- 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/

EI-ISAC

The EI-ISAC is federally funded by CISA and a division of the Center for Internet Security (CIS).

The EI-ISAC is autonomously guided by the Executive Committee and member organizations.


CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA
MS-ISAC®
Multi-State Information Sharing & Analysis Center®
Elections Infrastructure ISAC®
CIS

CISA focuses on the cybersecurity of all critical infrastructure within the United States (including election offices).

The MS-ISAC is a trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial (SLTT) government entities.

The EI-ISAC supports the rapidly changing cybersecurity needs of U.S. SLTT election offices.

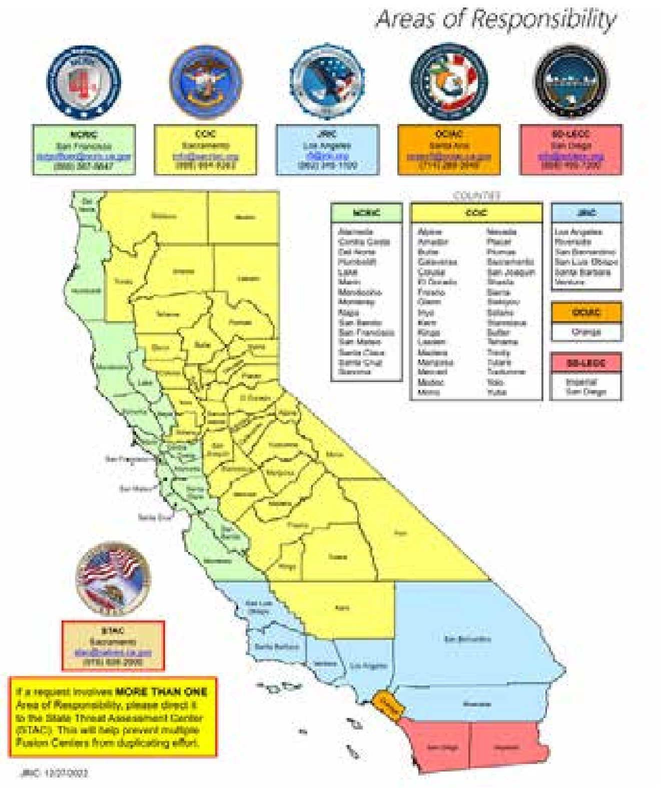
CIS is home to the MS-ISAC and the EI-ISAC

EI-ISAC

- Elections Infrastructure Information Sharing & Analysis Center
- Computer Incident Response Team (CIRT)
- The Security Operations Center (SOC) is available 24/7 to assist via phone or email:
- **866-787-4722**
- **soc@cisecurity.org**

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

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**

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.

Sampling of CISA’s Cybersecurity Offerings

- **Preparedness Activities**
  - Information / Threat Indicator Sharing
  - Cybersecurity Training and Awareness
  - Cyber Exercises and “Playbooks”
  - National Cyber Awareness System
  - Vulnerability Notes Database
  - Information Products and Recommended Practices
  - Cybersecurity Evaluations
    - Cyber Resilience Reviews (CRR™)
    - Cyber Infrastructure Surveys
    - Phishing Campaign Assessment
    - Vulnerability Scanning
    - Risk and Vulnerability Assessments (aka “Pen” Tests)
    - External Dependencies Management Reviews
    - Cyber Security Evaluation Tool (CSET™)
    - Validated Architecture Design Review (VADR)

- **Response Assistance**
  - Remote / On-Site Assistance
  - Malware Analysis
  - Hunt and Incident Response Teams
  - Incident Coordination

- **Cybersecurity Advisors**
  - Assessments
  - Working group collaboration
  - Best Practices private-public
  - Incident assistance coordination

- **Protective Security Advisors**
  - Assessments
  - Incident liaisons between government and private sector
  - Support for National Special Security Events

Range of Cybersecurity Assessments

STRATEGIC
(C-Suite Level)

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

TECHNICAL
(Network-Administrator
Level)

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)*

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: [illegible] IMPACT: [illegible] COMPLEXITY: [illegible] TACTIC, TECHNIQUE, AND PROCEDURE (TTP) OR RISK ADDRESSED: [illegible] RECOMMENDED ACTION: [illegible] FREE SERVICES AND REFERENCES: [illegible]	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: [illegible] IMPACT: [illegible] COMPLEXITY: [illegible] TTP OR RISK ADDRESSED: [illegible] RECOMMENDED ACTION: [illegible]	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: [illegible] IMPACT: [illegible] COMPLEXITY: [illegible] TTP OR RISK ADDRESSED: [illegible] RECOMMENDED ACTION: [illegible]	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: [illegible] IMPACT: [illegible] COMPLEXITY: [illegible] TTP OR RISK ADDRESSED: [illegible] RECOMMENDED ACTION: [illegible]	DATE: □ IMPLEMENTED □ IN PROGRESS □ SCOPED □ NOT STARTED	DATE: □ IMPLEMENTED □ IN PROGRESS □ SCOPED □ NOT STARTED	

CISA Cybersecurity Advisors (California)

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

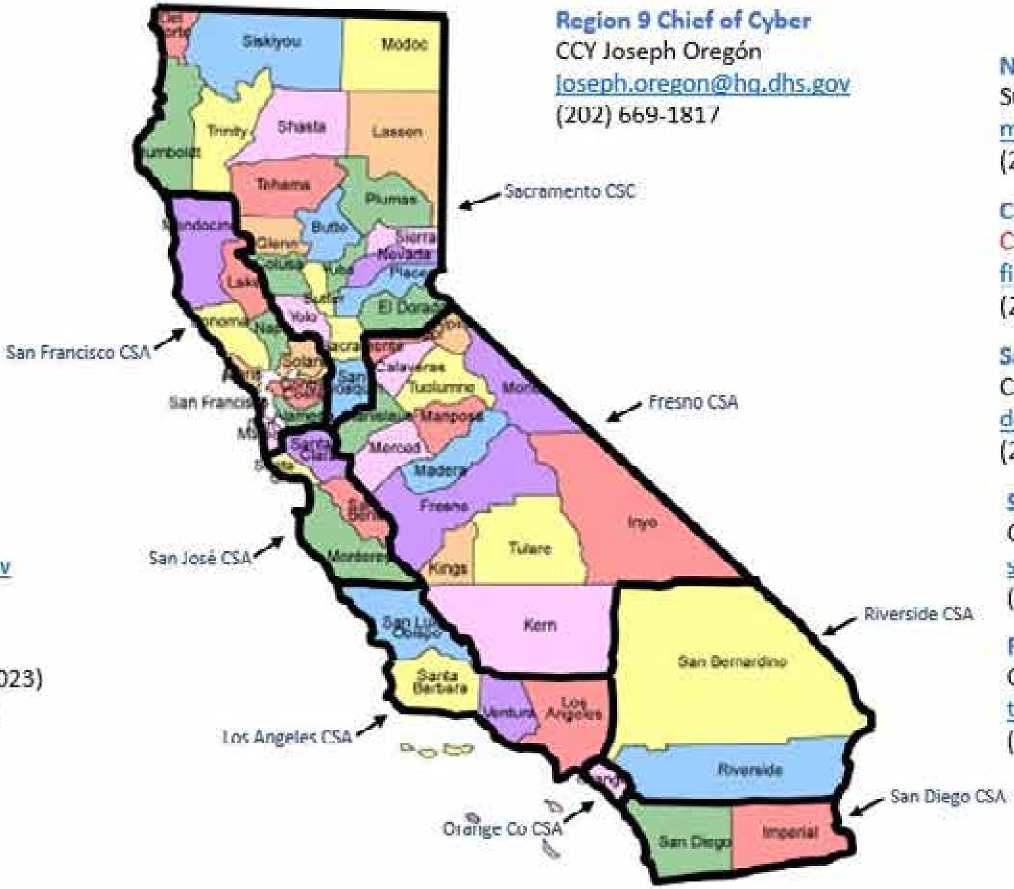
Los Angeles CSA
CSA Michael Kingsley
michael.kingsley@cisa.dhs.gov
202-834-8293

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 (10/10/2023)
Vincent.chapman@cisa.dhs.gov
(202) ###-####

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 (11/06/2023)
scott.alford@cisa.dhs.gov
(202) ###-####

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

Rev. 10/04/2023

Contact

General Inquiries

iodregionaloperations@cisa.dhs.gov

CISA Contact Information

Donald E. Hester Cybersecurity Advisor	Donald.Hester@cisa.dhs.gov +1 (202) 315-8091
Mario F. Garcia Supervisory Cybersecurity Advisor	Mario.Garcia@cisa.dhs.gov +1 (202) 309-1847

Cybersecurity and Infrastructure Security Agency

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA