Krishna Easton
Cybersecurity State Coordinator
Hawaii, American Samoa

Cybersecurity and Infrastructure Security Agency (CISA)

As America's Cyber Defense Agency and the National Coordinator for Critical Infrastructure Security and Resilience, CISA leads the national effort to understand, manage, and reduce risk to the cyber and physical infrastructure that Americans rely on every hour of every day.

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient infrastructure for the American people.

MISSION

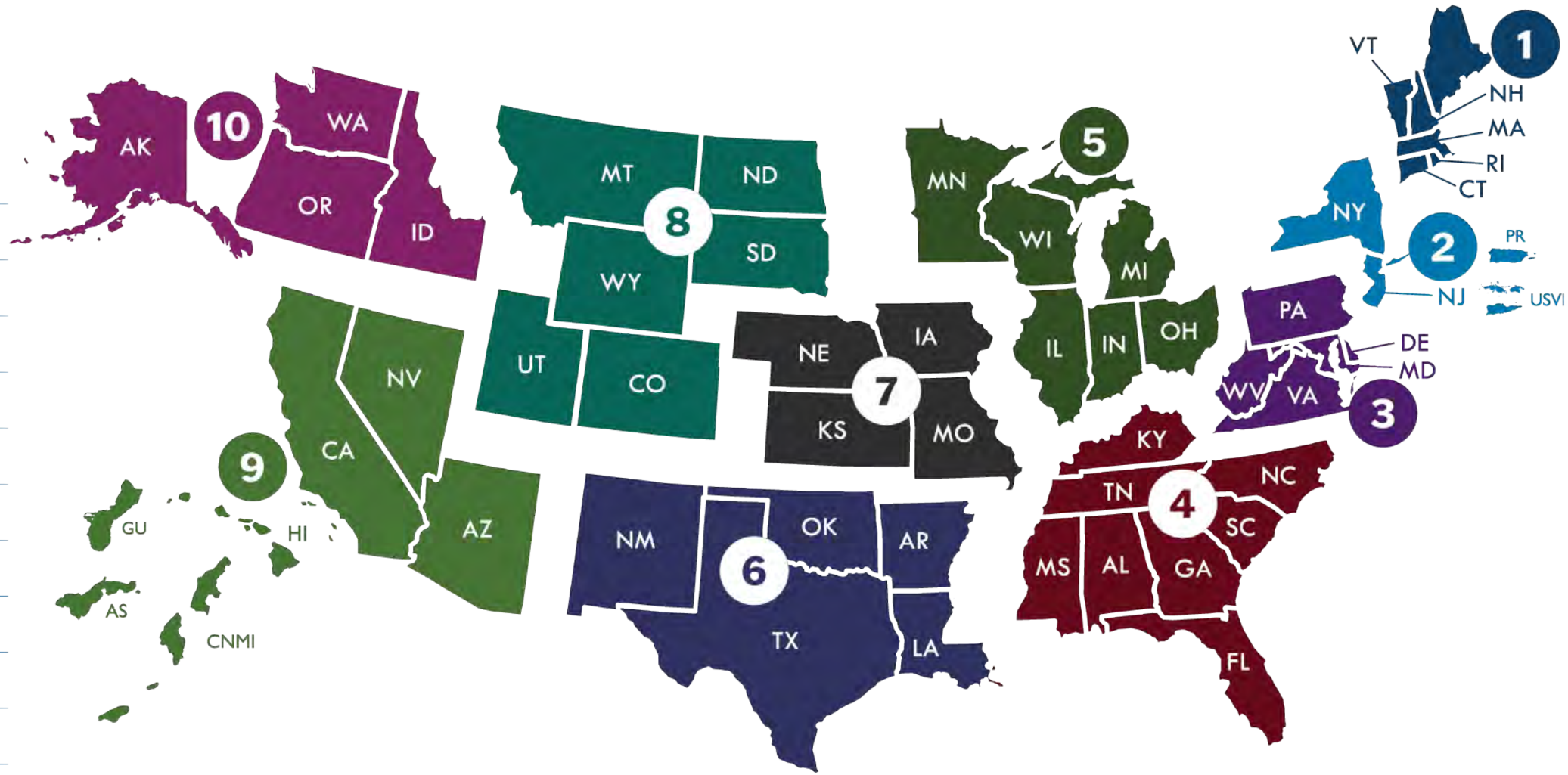
Lead the national effort to understand, manage, and reduce risk to the nation's cyber and physical infrastructure.

HTTPS://WWW.CISA.GOV

16 Critical Infrastructure Sectors & Corresponding Sector Risk Management Agencies

CISA Regions

- 1 Boston, MA
- 2 New York, NY
- 3 Philadelphia, PA
- 4 Atlanta, GA
- 5 Chicago, IL
- 6 Dallas, TX
- 7 Kansas City, MO
- 8 Denver, CO
- 9 Oakland, CA
- 10 Seattle, WA



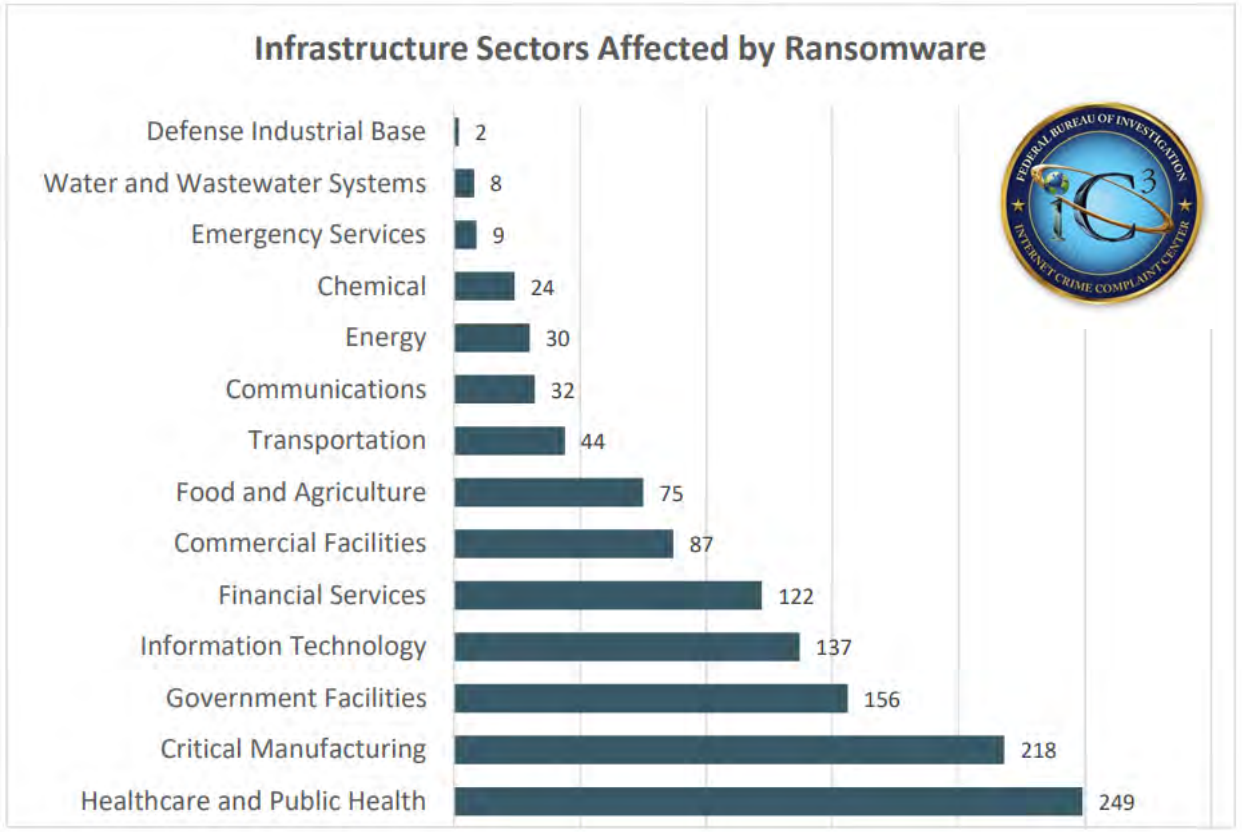
CISA.GOV/REGIONS


Today's Risk Landscape
ACTS OF TERRORISM
CYBER ATTACKS
EXTREME WEATHER
PANDEMICS
ACCIDENTS OR TECHNICAL FAILURES
Sophistication
THREATS
MOTIVATION
HACKTIVISM
Hacktivists use computer network exploitation to advance their political or social causes.
CRIME
Individuals and sophisticated criminal enterprises steal personal information and extort victims for financial gain.
INSIDER
Trusted insiders steal proprietary information for personal, financial, and ideological reasons.
ESPIONAGE
Nation-state actors conduct computer intrusions to steal sensitive state secrets and propriety information from private companies.
TERRORISM
Terrorist groups sabotage the computer systems that operate our critical infrastructure, such as the electric grid.
WARFARE
Nation-state actors sabotage military and critical infrastructure systems to gain an advantage in the event of conflict.

Risk Profile - Rich Target for Cyber Criminals

- Highly sensitive personal information
- Legacy mainframe systems and outdated technology stacks
- Tyranny of Distance
- Supply Chain and 3rd party Vendor Dependencies
- Advanced and emerging technology
  - Electronic health records system
  - Telehealth
  - Interoperability with clinical databases and EHRs
- Staff Training
- End Point Complexity
  - Large and diverse group of employees using/managing device
  - Centralized or decentralized equipment

Top Vulnerability Points Hospital Cyber Attacks



2023 Annual Report FBI Internet Crime Complaint Center (IC3)

- Ransomware Attacks: Malware encrypting sensitive data until a ransom amount is paid
- Phishing: Infecting seemingly innocuous emails with malicious links.
- Data Breaches: Unauthorized access to sensitive information.
- DDoS Attacks: Distributed denial-of-service attacks.

Healthcare Cyberattacks


BREAKING NEWS

Star Advertiser

Queen's Health Systems also affected after ransomware attack strikes Kronos software provider

By Peter Boylan

Dec. 14, 2021

[Queen's Health Systems also affected after ransomware attack strikes Kronos software provider]


UNIVERSITY of HAWAI'I–WEST O'AHU

Cyber

Ransomware Attack on the University of Vermont Health Network

By Edgar Namoca on March 4, 2021

[Ransomware Attack on the University of Vermont Health Network – Cyber]


DATA BREACHES

Hawaii Health Center Discloses Data Breach After Ransomware Attack

Community Clinic of Maui says a LockBit ransomware attack from earlier this year has resulted in a data breach impacting over 120,000 people.

By Eduard Kovacs
September 30, 2024

The Community Clinic of Maui in Hawaii, a nonprofit healthcare organization doing

TRENDING

[3,400 records accessed in DOH security breach | KHON2]

Timeline of the 2024 Change Healthcare Cyberattack

FEB. 21

- Optum reports connectivity issues.
- Change Healthcare experiences network threat and disconnects systems.

FEB. 26

- Ransomware group BlackCat claims responsibility for the attack.
- UnitedHealth reports that 90% of 70,000+ pharmacies modify claims processing.

MARCH 4

- AHA calls Change's funding program inadequate. Some providers start losing more than $100M a day.

MARCH 5

- HHS accelerates payments to affected hospitals and CMS urges payers to relax or remove prior authorizations.

MARCH 6

- UnitedHealth faces five federal lawsuits over the attack.

MARCH 12

- Payers reluctant to relax prior authorizations.
- AHIP President and CEO says removing prior authorizations could cause harm and fraud.

MARCH 13

- An investigation is launched into UnitedHealth and Change by the federal government.

MARCH 18

- Insurers meet with federal officials to discuss how to support providers still financially struggling after the cyberattack

- 190 million affected
- 25 days for medical claims
- 9 months-full clearinghouse services

*TechTarget - 2024 Top Healthcare Cyberattacks

Krishna Easton
March 23, 2025

Threat Actors Can Be Sophisticated…

But They Don’t Always Need To Be

Home | Information Security

CSO FROM IDG

ANALYSIS

Zero-days aren’t the problem -- patches are

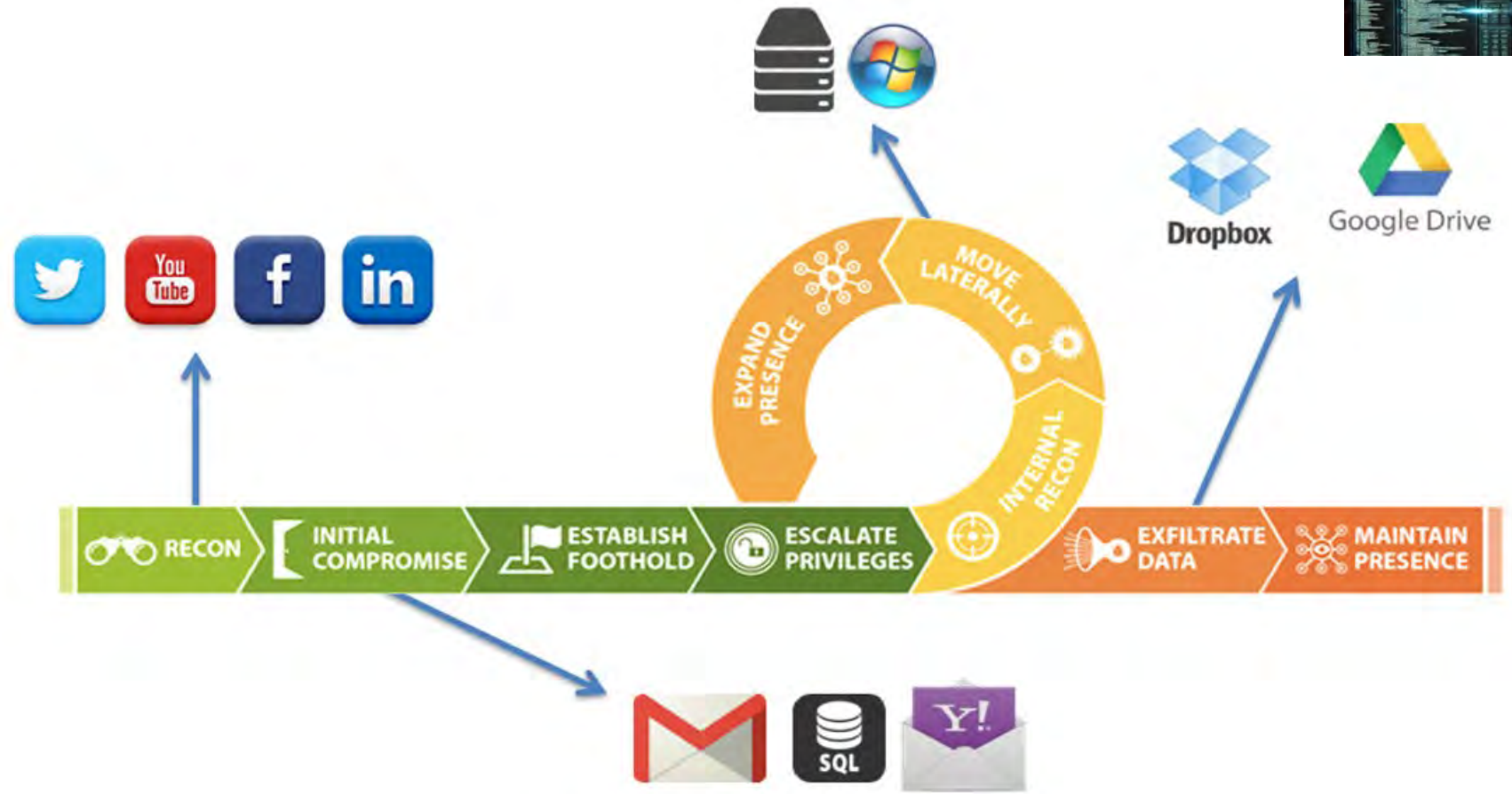
Everyone fears the zero-day exploit. But old, unpatched vulnerabilities still provide the means for malicious hackers to carry out the vast majority of hacks

https://www.csoonline.com/article/3075830/data-protection/zero-days-arent-the-problem-patches-are.html

. . .

Most hackers follow the path created by a very few smart ones -- and zero days make up a very small percentage of attacks. It turns out that patching vulnerable software, if implemented consistently, would stop most hackers cold and significantly reduce risk.

Cyber Attack Cycle



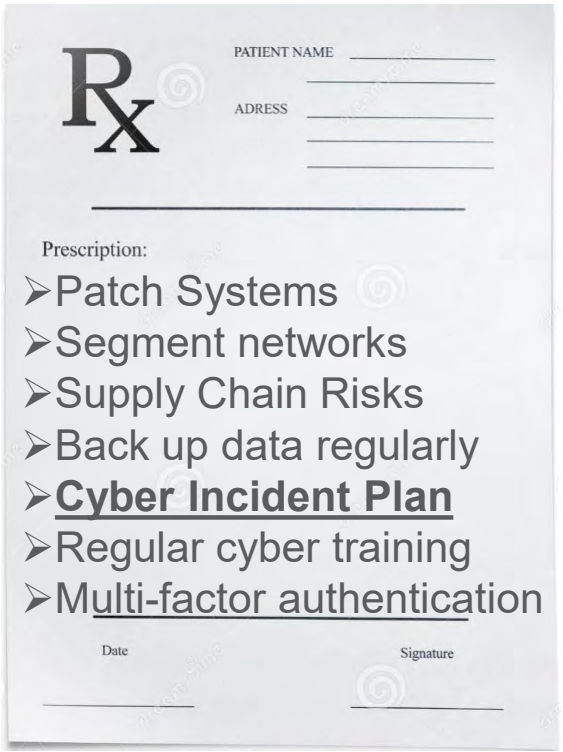
Legitimate business services can be used for illicit cyber acts

Cyber Prescription for the HPH Sector

➢Access CISA's Cyber Performance Goals and the Department of Health and Human Services' sector-specific cyber performance goals

https://www.cisa.gov/cybersecurity-performance-goals-cpgs

https://hhscyber.hhs.gov/performance-goals.html)



Range of Cybersecurity Assessments

- Cyber *Performance Goals (CPG)*
- *Ransomware Readiness Assessment (RRA)*
- *External Dependencies Management (EDM)*
- *Cyber Infrastructure Survey (CIS)*
- *Cyber Resilience Review (CRR)*
- *Tabletop Exercises (TTX)*
- *Cyber Hygiene Services*
  - *Vulnerability & Web Application Scanning*
- *Validated Architecture Design Review (VADR)*
- *Remote Penetration Test (RPT)*
- *Risk and Vulnerability Assessment (RVA)*

Ransomware Readiness Assessment

- ✓ Backup and Recovery Process
- ✓ Develop Incident Management & Response Plan
  - ✓ Confirm you Have up-to-date Points of Contact on File
- ✓ Update Software and Operating Systems with the Latest Patches & Versions
- ✓ Apply the Principle of Least Privilege to all Systems and Services
- ✓ Secure End Users Against Phishing and Social Engineering
- ✓ Email Security Measures
  - ✓ Scan incoming and outgoing emails
  - ✓ Implement spoofing prevention measures
- ✓ Consider Leveraging Endpoint and Network Security Devices

https://stopransomware.gov

Additional Available Resources

- CISA's cybersecurity advisories

  Cybersecurity Alerts & Advisories | CISA

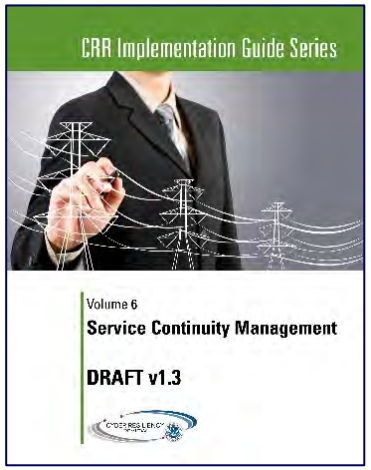
  2023 Top Routinely Exploited Vulnerabilities

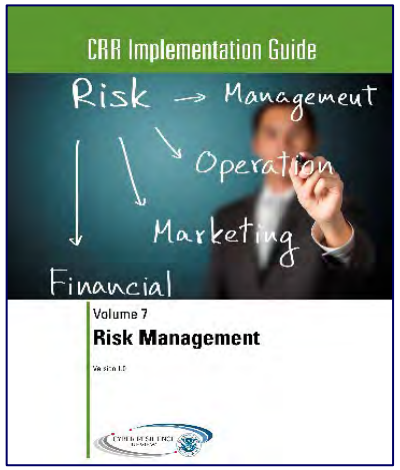
- Secure Our World resources to promote basic cybersecurity best practices

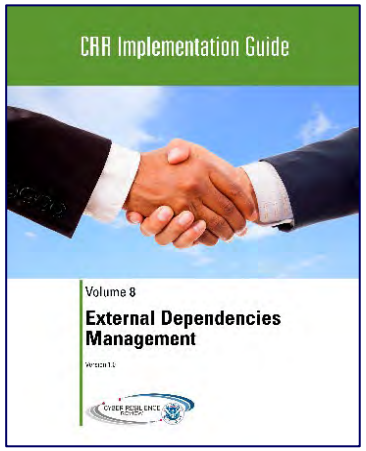
  Secure Our World | CISA

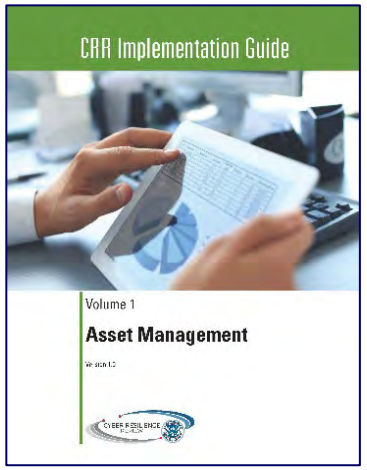
- Information and Communications Technology (ICT) supply chain risk management resources

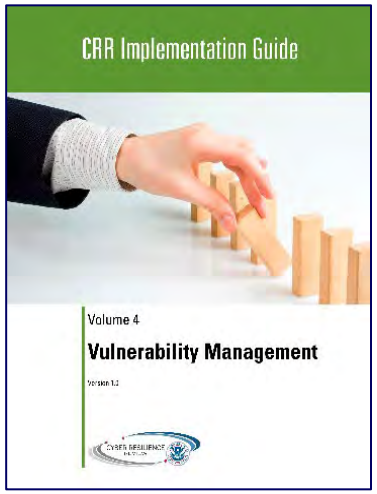
  ICT Supply Chain Risk Management Task Force | CISA











Cyber or Physical Tabletop Exercises

Develop and conduct cybersecurity-based scenarios that incorporate various cyber threat vectors including Ransomware, insider threats and phishing exercise

- Customized and Facilitated Exercises
- Tabletop Exercise Packages (CTEPs)
  - Off-the-shelf, do it yourself
- Small-scale Discussion-based
- Large-scale Operations-based Exercises

CISA Tabletop Exercise Packages | CISA

International Outreach

- CISA is an official partner of the Pacific Cyber Security Operational Network (PaCSON)
  - Operational cybersecurity network consisting of regional working-level cyber security and technical experts from eligible governments across the Pacific.
  - Not a Computer Emergency Response Team (CERT) or Computer Security Incident Response Team (CSIRT) and does not provide an Incident Response (IR) capability.
  - Maintains an operational cyber security points of contact and empowers members to share cyber security threat information; provides opportunities for technical experts to share tools, techniques and ideas; and is an enabler of cooperation and collaboration, particularly where a cyber security incident affects the region.
- CISA partners with other nations such as Japan, Australia, and New Zealand on capacity building programs.

IA-IndoPac@mail.cisa.dhs.gov

PaCSON
PACIFIC CYBER SECURITY OPERATIONAL NETWORK

InfraGard Hawaii Members Alliance

InfraGard is a partnership between the FBI and members of the private sector for the protection of U.S. Critical Infrastructure.

AN ALLIANCE FOR NATIONAL INFRASTRUCTURE PROTECTION

https://Infragard.org

Krishna Easton
March 23, 2025

CISA Central

CISA Central works to reduce the risk of systemic cybersecurity and communications challenges in our role as the Nation's flagship cyber defense, incident response, and operational integration center.

- Most centralized way for partners and stakeholders to engage with CISA
- Request CISA assistance and get information on current activity and threat landscape
- Central coordinates cyber activities with homeland security, law enforcement, intelligence, and defense communities
- Manages CISA 24/7 operations center

Central@cisa.dhs.gov

SayCISA@cisa.dhs.gov

1-844-Say-CISA

Region 9 Pacific Islands CSA Team

- **Veronica Mitchell**
  Supervisory Cybersecurity Security Advisor (Pacific Coast)
  Cybersecurity and Infrastructure Security Agency (CISA)
  Cell: (202) 664-2097| Email: veronica.mitchell@cisa.dhs.gov
- **Giovanni Williams**
  Cybersecurity Security Advisor Lead (Hawaii, American Samoa)
  Cybersecurity and Infrastructure Security Agency (CISA)
  Cell: (202) 503-5614| Email: giovanni.williams@cisa.dhs.gov
- **Krishna Easton**
  Cybersecurity State Coordinator (Hawaii, American Samoa)
  Cybersecurity and Infrastructure Security Agency (CISA)
  Cell: (717) 219-8283 | Email: krishna.easton@cisa.dhs.gov
- **Joseph Oregón**
  Cybersecurity Security Advisor, Region 9
  Cybersecurity and Infrastructure Security Agency (CISA)
  Cell: (202) 669-1817 | Email: joseph.oregon@hq.dhs.gov
- **Jennilyn LaBrunda**
  Cybersecurity Security Advisor (Guam, Northern Mariana Islands)
  Cybersecurity and Infrastructure Security Agency (CISA)
  Cell: (808) 260-3143 | Email: jennilyn.labrunda@cisa.dhs.gov

- **Supported State/Territories:**
  Hawaii
  Guam
  Northern Mariana Islands
  American Samoa

For more information:
www.cisa.gov

CISA International Affairs:
IA-IndoPac@mail.cisa.dhs.gov

CISA Region 9 Office: CISARegion9@cisa.dhs.gov

CISA Central 24/7: 888-282-0870

Report incidents: Report@cisa.gov

Additional information: Central@cisa.dhs.gov

Visit **CISA.gov** to learn more and see our mission in action at **cisa.gov/about/2023YIR**
or contact us at **central@cisa.dhs.gov**