AMERICAN PUBLIC WORKS ASSOCIATION CLICK, LISTEN, AND LEARN

Joseph Larkin & David Lee
June 22, 2023

Cybersecurity and Infrastructure Security Agency

CISA works with partners to defend against today's threats and collaborate to build a more secure and resilient infrastructure for the future.

CISA is the operational lead for federal cybersecurity and the national coordinator for critical infrastructure security and resilience. We are designed for collaboration and partnership.

Our Mission: Lead the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure.

Our Vision: Secure and resilient infrastructure for the American people.

Cybersecurity and Infrastructure Security Agency Goals

GOAL 1 CYBER DEFENSE

Spearhead the national effort to ensure defense and resilience of cyberspace

GOAL 2 RISK REDUCTION AND RESILIENCE

Reduce risks to, and strengthen resilience of, America’s critical infrastructure

GOAL 3 OPERATIONAL COLLABORATION

Strengthen whole-of-nation operational collaboration and information sharing

GOAL 4 AGENCY UNIFICATION

Unify as One CISA through integrated functions, capabilities, and workforce

Cybersecurity and Infrastructure Security Agency Divisions

Cybersecurity Division

Emergency Communications Division

Infrastructure Security Division

Integrated Operations Division

National Risk Management Center

Stakeholder Engagement Division

Emergency Services Sector Risk Management Agency

CISA serves as the Sector Risk Management Agency (SRMA) for the Emergency Services Sector and offers many resources and training materials to help manage risks, improve security, and aid the implementation and execution of protective measures across this sector.

The Emergency Services Sector Management Team (SMT) manages CISA’s relationships with, and performs the SRMA function for, the Emergency Services Sector.

Emergency Services Sector Overview

The mission of the Emergency Services Sector (ESS) is to save lives, protect property and the environment, assist communities impacted by disasters, and aid recovery during emergencies.

Five distinct disciplines compose the ESS, encompassing a wide range of emergency response functions and roles. In addition to Public Works is Law Enforcement, Fire and Rescue Services, Emergency Medical Services, and Emergency Management.

These disciplines include various specialized capabilities.

CISA Cybersecurity Resources - AES

The **Assessment Evaluation and Standardization (AES)** program enables organizations to have a trained individual that can perform several cybersecurity assessments and reviews in accordance with industry and/or federal information security standards. AES courses include:

- High Value Assets (HVA) Course
- Cyber Resilience Review (CRR) Course
- External Dependencies Management (EDM) Course
- Risk and Vulnerability Assessment (RVA) Course
- Cybersecurity Performance Goals (CPG) Course
- Validated Architecture Design Review (VADR) Course
- Incident Management Review (IMR) Course

CISA Cybersecurity Resources - VS

Vulnerability Scanning (VS) evaluates external network presence by executing continuous scans of public, static IPv4s for accessible services and vulnerabilities and assesses the health of your internet-accessible assets by checking for known vulnerabilities, weak configurations—or configuration errors—and suboptimal security practices. VS service also recommends ways to enhance security through modern web and email standards. This service includes Target Discovery—identifies all active internet-accessible assets (networks, systems, and hosts) to be scanned—and Vulnerability Scanning—initiates non-intrusive checks to identify potential vulnerabilities and configuration weaknesses—and provides weekly vulnerability reports and ad-hoc alerts.

CISA Cybersecurity Resources - CRR Interview

The **Cyber Resilience Review (CRR)** is an interview-based assessment that evaluates an organization’s operational resilience and cybersecurity practices across the following 10 domains: Asset Management, Controls Management, Configuration and Change Management, Vulnerability Management, Incident Management, Service Continuity Management, Risk Management, External Dependency Management, Training and Awareness, and Situational Awareness. Receiving a Cyber Resilience Review will provide:

- Improved enterprise-wide awareness of the need for effective cybersecurity management
- A review of capabilities essential to the continuity of critical services during operational challenges and crisis
- Integrated peer performance comparisons for each of the 10 domains covered in the assessment
- A comprehensive final report that includes options for improvement.

CISA Cybersecurity Resources - CRR Self-Assessment

The **Cyber Resilience Review (CRR)** is also available as a self-assessment. These guides were developed for organizations that have participated in a CRR but are useful to any organization interested in implementing or maturing operational resilience capabilities for critical cyber dependent services.

- CRR Self-Assessment so that a user can employ the CRR for self-evaluation purposes for their organization, leverage it prior to an onsite assessment facilitated by a DHS Cybersecurity professional.
- CRR User Guide contains the overall description of the CRR along with detailed steps and explanations for how to conduct a CRR self-assessment.
- CRR Question Set with Guidance contains the entire CRR self-assessment question set along with guidance on how to interpret and answer each of the questions.
- CRR NIST Framework Crosswalk provides a cross-reference chart for each of the categories in the NIST Cybersecurity Framework and how they align to the CRR.

CISA Cybersecurity Resources - EDM

The **External Dependencies Management (EDM) Assessment** evaluates an organization’s management of external dependencies. The EDM Assessment evaluates the maturity and capacity of an organization’s risk management across the following areas: Relationship Formation, Relationship Management and Governance, and Service Protection and Sustainment. Available for download are:

- EDM Assessment so that a user can employ the EDM assessment for self-evaluation purposes.
- EDM User Guide contains the overall description of the EDM along with detailed steps and explanations for how to conduct an EDM self-assessment.
- EDM Primary Guidance contains the entire EDM assessment question set along with guidance on how to interpret and answer each of the questions.
- EDM NIST Cyber Security Framework Crosswalk provides a cross-reference chart for each of the categories in the NIST Cybersecurity Framework and how they align to the EDM.

CISA Cybersecurity Resources - CIS

The **Cyber Infrastructure Survey** evaluates the effectiveness of organizational security controls, cybersecurity preparedness, and the overall resilience of an organization's cybersecurity ecosystem. This survey provides a service-based view opposed to a programmatic view of cybersecurity. An organization's critical services are assessed against more than 80 cybersecurity controls grouped into the following 5 top-level domains: Cybersecurity Management, Cybersecurity Forces, Cybersecurity Controls, Cybersecurity Incident Response, and Cybersecurity Dependencies. Completing the Cyber Infrastructure Survey will provide an organization with the following:

- Effective assessment of critical service cybersecurity controls
- Interactive dashboard to support cybersecurity planning and resource allocation
- Peer performance data visually depicted on the dashboard

CISA Cybersecurity Resources - CSET

The **Cyber Security Evaluation Tool (CSET)** is a stand-alone desktop application that guides asset owners and operators through a systematic process of evaluating Operational Technology and Information Technology. After completing the evaluation, the organization will receive reports that present the assessment results in both a summarized and detailed manner. It includes the Cyber Resilience Review, Cyber Infrastructure Survey, and the new Ransomware Readiness Assessment (RRA). The RRA is a self-assessment based on a tiered set of practices to help organizations better assess how well they are equipped to defend and recover from a ransomware incident.

CISA Physical Security Resources - AV

Assist Visits, conducted by Protective Security Advisors (PSAs) with critical infrastructure facility representatives. are a cornerstone of the voluntary outreach effort to critical infrastructure owners and operators. An Assist Visit:

- Establishes and enhances the DHS relationship with critical infrastructure owners and operators.
- Informs them of the importance of their facility.
- Explains how their facility or service fits into its specific critical infrastructure sector.
- Provides an overview of the CISA resources available to the facility to enhance security and resilience.
- Reinforces the need for continued vigilance.

During an Assist Visit, PSAs focus on coordination, outreach, training, and education.

CISA Physical Security Resources - IST

The **Infrastructure Survey Tool (IST)** is a voluntary, web-based assessment to identify and document the overall security and resilience of a facility. The IST focuses on:

Identifying facilities' physical security, security forces, security management, information sharing, protective measures, and dependencies related to preparedness, mitigation, response, resilience, and recovery;

- Identifying security areas of possible improvements;
- Creating facility protective and resilience measures indices that show a comparison to similar facilities that have completed ISTs; and
- Tracking progress toward improving critical infrastructure security.

CISA provides the assessment information that the IST collects and analyzes to owners and operators via both a written report and the IST Dashboard, which is accessed through a secure web portal.

CISA Physical Security Resources - RRAP

The **Regional Resiliency Assessment Program (RRAP)** is a voluntary, cooperative assessment of specific critical infrastructure that identifies a range of security and resilience issues that could have regionally or nationally significant consequences. The goal of the RRAP is to generate understanding and action among public and private sector partners to improve the resilience of a region’s critical infrastructure. Each RRAP project typically involves a year-long process to collect and analyze data on the critical infrastructure within the designated area, followed by continued technical assistance to enhance the infrastructure's resilience. The goals of the RRAP include:

- Resolve infrastructure security and resilience knowledge gaps
- Inform risk management decisions
- Identify opportunities and strategies to enhance infrastructure resilience
- Improve critical partnerships among the public and private sectors

CISA Physical Security Resources - OBP

The **Office for Bombing Prevention (OBP)** develops and delivers a diverse curriculum of training and awareness products to build nationwide counter-improvised explosive device (C-IED) core capabilities and enhance awareness of terrorist threats. OBP offers bombing prevention training throughout the United States to meet stakeholder needs.

- In-person in a traditional classroom setting
- In-residence at the Federal Emergency Management Agency's (FEMA) Center for Domestic Preparedness (CDP)
- Online through a Virtual Instructor-Led Training (VILT) platform and through Independent Study Training (IST)

OBP provides a wide array of awareness products - cards, posters, checklists, guides, videos, briefings, and applications - with C-IED awareness information for the general public and critical infrastructure to prevent, protect against, respond to, and mitigate bombing incidents.

CISA Services Catalog

The CISA Services Catalog is a single resource that provides users with access to information on services across all of CISA’s mission areas that are available to Federal Government; State, Local, Tribal and Territorial Government; Private Industry; Academia; NGO and Non-Profit; and General Public stakeholders. The catalog is interactive, allowing users to filter and quickly hone in on applicable services with just a few clicks. Users can search based on topic, audience, and readiness level.

Free Cybersecurity Services and Tools - Foundational

CISA has compiled a list of free cybersecurity tools and services to help organizations further advance their security capabilities, including cybersecurity services provided by CISA, widely used open-source tools, and free tools and services offered by private and public sector organizations across the cybersecurity community.

All organizations should take certain **foundational measures** to implement a strong cybersecurity program:

- Fix the known security flaws in software.
- Implement multifactor authentication (MFA).
- Halt bad practices.
- Sign up for CISA’s Cyber Hygiene Vulnerability Scanning.
- Get your Stuff Off Search (S.O.S.).

Free Cybersecurity Services and Tools

After making progress on the foundational measures, organizations can use the free services and tools listed below to mature their cybersecurity risk management. These resources are categorized according to the four goals outlined in *CISA Insights: Implement Cybersecurity Measures Now to Protect Against Critical Threats*:

- Reduce the likelihood of a damaging cyber intrusion (89 items)
- Take steps to quickly detect a potential intrusion (38 items)
- Ensure that the organization is prepared to respond if an intrusion occurs (13 items)
- Maximize the organization's resilience to a destructive cyber incident (12 items)

Emergency Services SMT Resources - SSP & Profile

The **Emergency Services Sector-Specific Plan** details how the National Infrastructure Protection Plan (NIPP) 2013 risk management framework is implemented within the context of the unique characteristics and risk landscape of the sector.

The **Emergency Services Sector Profile** presents a picture of the Emergency Services Sector as a whole and opens an avenue to greater federal and sector partner coordination regarding emergency services discipline definitions; national census and data collection methods; and community awareness of capabilities, dependencies, and interdependencies.

Emergency Services SMT Resources - Landscape

The **Emergency Services Sector Landscape** details the multiple factors that may affect the security and resilience posture of the Emergency Services Sector. These factors, which influence the current operating environment and associated decision-making processes, stem from environmental, technological, human, and physical causes. As the Emergency Services Sector focuses on protecting other sectors and the public, unique challenges arise in addressing the security and resilience of the Emergency Services Sector as critical infrastructure.

Emergency Services SMT Resources - CPS & ASG

The **Emergency Services Sector Continuity Planning Suite** provides a centralized collection of existing guidance, processes, products, tools, and best practices to support the development and maturation of continuity planning for the first responder community.

The **Emergency Services Sector Active Shooter Guide** provides emergency services personnel with the basic building blocks for developing an Active Shooter Program with communities. This guide highlights resources and planning considerations, which will enhance emergency services organizations' ability to develop or improve community planning and preparedness for active shooter incidents.

Emergency Services SMT Resources - HSIN-ES & InfoGram

Managed by the Emergency Management and Response-Information Sharing and Analysis Center (EMR-ISAC), the **Homeland Security Information Network - Emergency Services (HSIN-ES)** contains a repository of FOUO and LES documents on a variety of topics including CBRNE, Cybersecurity, Emerging Threats, Partner Products, Public Health, and Transportation.

Produced weekly, the **InfoGram** includes short articles about the protection of community critical infrastructures and emergency responders.

CISA Regions

CISA's program of work is carried out across the nation by personnel assigned to its 10 regional offices.

Region 1 - CT, ME, MA, NH, RI, VT

Region 2 - NJ, NY, PR, USVI

Region 3 - DE, DC, MD, PA, VA, WV

Region 4 - AL, FL, GA, KY, MS, NC, SC, TN

Region 5 - IL, IN, MI, MN, OH, WI

Region 6 - AR, LA, NM, OK, TX

Region 7 - IA, KS, MO, NE

Region 8 - CO, MT, ND, SD, UT, WY

Region 9 - AZ, CA, HI, NV, GU, AS, CNMI

Region 10 - AK, ID, OR, WA

Within each CISA Region are your local and regional Protective Security Advisors (PSAs), Cyber Security Advisors (CSAs), Emergency Communications Coordinators (ECCs), and Chemical Security Inspectors (CSIs). In order to build stakeholder resiliency and form partnerships, these field personnel assess, advise, and assist and provide a variety of risk management and response services.

For more information:

www.cisa.gov/Emergency-Services-Sector

Questions?

EmergencyServicesSector@cisa.dhs.gov

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA