IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

CYBER RESILIENCY RESOURCES FOR PUBLIC SAFETY

As cyber threats and vulnerabilities grow in complexity and sophistication, cyber incidents have become one of the greatest operational risks to public safety.

Achieving secure and resilient voice and data communications is essential for agencies to execute their missions. Advanced planning is a key component of an agency's cybersecurity program—by developing and maintaining cybersecurity risk management and evolving security requirements, public safety agencies are better prepared to prevent or mitigate the effects of a cyber incident

Resiliency is defined as "…the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents…"[1]

CYBERSECURITY FOR PUBLIC SAFETY

According to the 2018 SAFECOM Nationwide Survey, respondents:[2,3]

47% Indicated that **cybersecurity incidents have had an impact on the ability of their emergency response providers** and government officials' ability to communicate over the past five years

36% Indicated that **they have not yet instituted cybersecurity best practices**, such as risk assessments, continuous monitoring, and identity management

Despite every effort, cyber incidents will occur. As a result, it is essential for public safety agencies to find ways to detect threats, execute response procedures, implement mitigation efforts, and eradicate the cause of the incident.

Establishing a cybersecurity risk management program can help organizations identify and prioritize risks, protect resources, detect threats, and enable coordinated response and recovery efforts.[4] Determining strategies to increase the resiliency of public safety networks and the knowledge of personnel who administer them can help prevent the loss of critical communications.

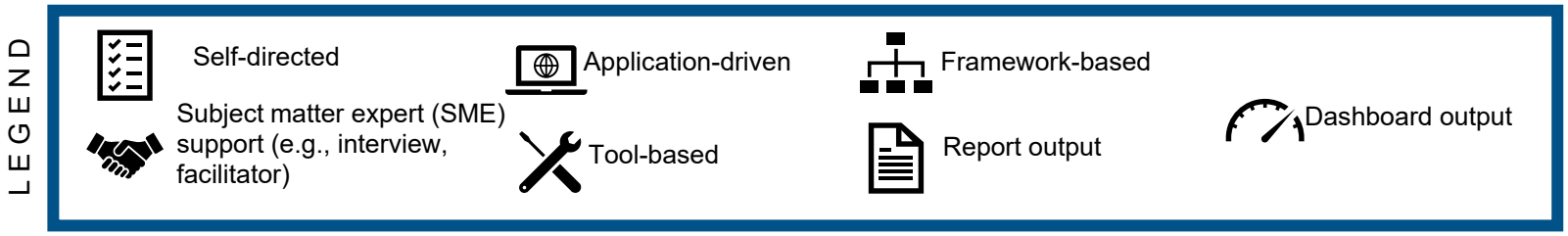
Cybersecurity is a dynamic process of assessing risk and enhancing defense. As a result, the public safety community must work continually to identify risks and address evolving security requirements as a means of protecting their mission critical networks.

ASSESSING RESILIENCY

Cybersecurity is a shared mission across all levels of government, the private sector, nongovernmental organizations, and the public. In this context, organizations must take proactive measures to enhance their overall cybersecurity posture.

The Cybersecurity and Infrastructure Security Agency (CISA) has compiled the following cyber resiliency resources provided by the federal government, industry, and trade associations. The availability and cost associated with any resource is subject to change at any time.

CISA CYBER RESILIENCY RESOURCES



NAME	OVERVIEW
Advanced Malware Analysis Center (AMAC)	The AMAC provides 24/7 dynamic analysis of malicious code. Stakeholders submit samples via an online website and receive a technical document outlining analysis results. Experts detail recommendations for malware removal and recovery activities. This service can be performed in conjunction with incident response services if required. Service benefits include an isolated network, classified capability, analytical capabilities, and extrication of malicious code. **Sources:** • CISA Detection and Prevention • U.S. Computer Emergency Readiness Team (US-CERT) AMAC Malware Analysis Submissions
CISA Central	CISA Central is a one-stop-shop for information sharing and situational awareness monitoring. CISA Central consolidates the people, processes, and technology for operations and information sharing activities within CISA under a single team. This includes certain functions of the former National Cybersecurity and Communications Integration Center (NCCIC), National Infrastructure Coordinating Center (NICC), and National Coordinating Center for Communications (NCC). **Source:** • CISA Central
Communications and Cyber Resiliency Toolkit	CISA developed the *Public Safety Communications and Cyber Resiliency Toolkit* as a collection of resources to assist public safety agencies and others responsible for communications networks in evaluating current resiliency capabilities, identifying ways to improve resiliency, and developing plans for mitigating the effects of potential resiliency threats. To facilitate viewing available resources, the toolkit includes an interactive graphic. Topic specific systems-based resources appear as building shapes (blue) and threats are cloud shapes (red). Clicking on a topic reveals a list of resources accompanied by a brief description. **Source:** • Communications and Cyber Resiliency Toolkit
Cyber Essentials	The *Cyber Essentials* campaign is designed to help organizations understand and address cybersecurity risk, and equip them with basic steps and resources to improve their cybersecurity. *Cyber Essentials* includes two parts: (1) guiding principles for leaders to develop a culture of security; and (2) specific actions for leaders and their information technology (IT) professionals to put that culture into action, all with the aim of a better defensive position against commonplace cybersecurity threats. **Source:** • CISA Cyber Essentials

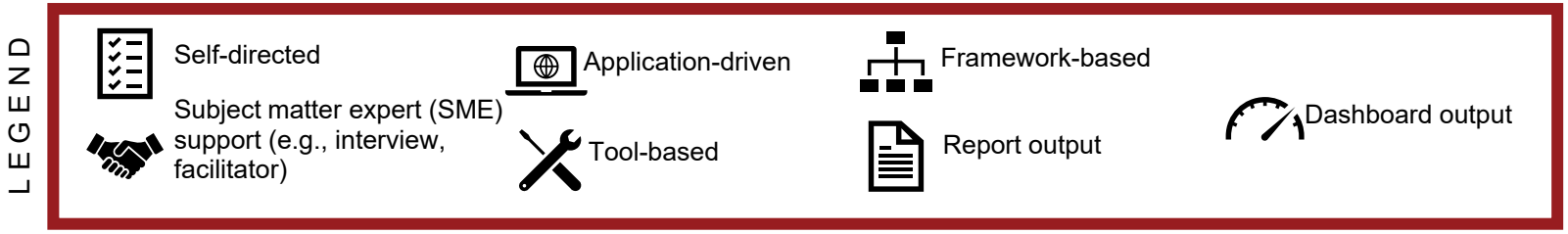
NAME	OVERVIEW
Cyber Infrastructure Survey 	This survey evaluates the effectiveness of organizational security controls, cybersecurity preparedness, and overall resilience. The Cyber Infrastructure Survey assesses critical services against more than 80 cybersecurity controls grouped under five top-level domains (i.e., cybersecurity management, cybersecurity forces, cybersecurity controls, cyber incident response, and cyber dependencies). Following the assessment, organizations are provided with a dashboard to compare results against industry peers; review data in the context of specific cyber and physical threat scenarios; and adjust the importance of in-place practices to observe the effects on overall cyber posture. The survey takes approximately four hours to complete. The Chief Information Security Officers (CISOs), Industrial Control Systems (ICS)/Supervisory Control and Data Acquisition (SCADA) security managers, and IT security managers are required to perform the assessment. **Source:** • CISA Cyber Resource Hub • CISA Services Catalog
Cyber Resilience Review (CRR) 	The CRR evaluates operational resilience and cybersecurity capabilities. Based on the CERT Resilience Management Model, the CRR enables an organization to assess its capabilities relative to the *National Institute of Standards and Technology (NIST) Cybersecurity Framework* and a crosswalk document that maps the CRR to the NIST framework is included as a component of the CRR self-assessment package. The CRR seeks participation from a cross-functional team consisting of representatives from an organization's business, operations, security, IT, and maintenance areas. The CRR takes one business day to complete. Organizations have two options in conducting a CRR: (1) a self-assessment available for download; or (2) an on-site facilitated session with trained CISA representatives. The CRR report is created exclusively for an organization's internal use. **Source:** • CISA Cyber Resource Hub
Cybersecurity Advisor (CSA) Program 	CSAs help prepare and protect private sector entities and state, local, tribal, and territorial (SLTT) governments from cybersecurity threats. CSAs promote cybersecurity preparedness, risk mitigation, and incident response capabilities, working to engage stakeholders through partnership and direct assistance activities. CSAs are distributed personnel assigned to 10 regions throughout the U.S., which are aligned to the Federal Emergency Management Agency (FEMA) regions. CSAs engage organizations in order to cultivate partnerships, deliver cybersecurity services, and create channels of communication to Department of Homeland Security (DHS) cyber programs and Department leadership. CSAs offer cyber preparedness, strategic messaging, working group support, partnership development, cyber assessments, and incident coordination and support services. **Source:** • CISA Stakeholder Engagement and Cyber Infrastructure Resilience—Best Practices: Cybersecurity Advisors

NAME	OVERVIEW
Cybersecurity Assessment and Risk Management Approach (CARMA) 	CARMA assists public and private sector partners in assessing, prioritizing, and managing cyber infrastructure threats. The assessment provides a national-level, sector-specific profile for critical infrastructure owners and operators as they use a framework to identify cyber risks and determine the appropriate response. CARMA's process encompasses the full risk management cycle: Stage I (Scope Risk Management Activities), Stage II (Identify Cyber Infrastructure), Stage III (Conduct Cyber Risk Assessment), Stage IV (Develop Cyber Risk Management Strategy), and Stage V (Implement Strategy and Measure Effectiveness). **Sources:** • CISA Emergency Services Sector Cybersecurity Initiative • CISA Emergency Services Sector Cyber Risk Assessment Factsheet
Cybersecurity Evaluation Tool (CSET®) 	To evaluate operational readiness, this application asks asset owners and operators a series of detailed questions about their operational technology (OT) and IT network security practices, system components, and network architectures. These questions are derived from industry-recognized cybersecurity standards. Following the questionnaire, CSET provides a dashboard highlighting areas of strength and weakness, allowing users to compare trends across multiple assessments. The tool also includes recommendations to help organizations better preempt a cybersecurity attack. **Source:** • CISA Cyber Resource Hub
Enhanced Cybersecurity Services (ECS) 	The ECS program facilitates the protection of IT networks by offering intrusion detection and prevention services through approved service providers. All U.S.-based public or private entities, including SLTT organizations, are eligible to participate. The two primary ECS services are Domain Name System (DNS) sinkholing and email filtering. These services block possible malware communications and spear phishing campaigns targeting networks. Participating in ECS affords organizations a quick and efficient way to receive protections that use classified information to thwart possible malicious communications and spear phishing campaigns without having to meet the otherwise burdensome requirements of maintaining secure facilities and employing cleared personnel. **Sources:** • CISA Detection and Prevention • CISA Enhanced Cybersecurity Services
Remote Penetration Testing (RPT) 	RPT uses a dedicated remote team to assess, identify, and mitigate vulnerabilities to exploitable pathways. RPT focuses entirely on externally accessible systems and may include methodologies such as scenario-based external network penetration testing, external web application testing, and PCAs. After completing an RPT, a final report is generated that includes business executive recommendations, specific findings and potential mitigations, as well as technical attack path details. An optional debriefing presentation summarizing preliminary findings and observations is also available. **Source:** • CISA Cyber Resource Hub

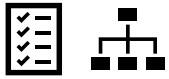
NAME	OVERVIEW
External Dependencies Management (EDM) Assessment 	The EDM assessment is used to evaluate an organization's management of their external dependencies within the information and communications technology (ICT) supply chain. Specifically, the assessment evaluates the relationship between an organization's high-value services and assets (i.e., people, technology, facilities, and information) and how risks are managed when supporting these services. Stakeholders use EDM assessments to evaluate their maturity and capacity to manage risks across three areas: (1) relationship formation; (2) relationship management and governance; and (3) service protection and sustainment. The EDM report is created exclusively for an organization's internal use and takes approximately four hours to complete. Representatives responsible for IT policy and governance, IT security planning and management, IT infrastructure, IT operations, business operations, business continuity and disaster recovery planning, risk management, procurement, and vendor management are needed to perform the assessment. **Sources:** • CISA Cyber Resource Hub • CISA Assessments: Cyber Resilience Review—CRR Resource Guides—External Dependencies Management
Federal Virtual Training Environment (FedVTE) 	The FedVTE content library contains pre-recorded classroom cybersecurity training for SLTT government personnel, federal government personnel and contractors. FedVTE provides government-wide, online, and on-demand access to cybersecurity training to help the workforce maintain expertise and foster operational readiness. With courses ranging from beginner to advanced levels, the system is available at no cost to users, and is accessible from any internet-enabled computer. **Source:** • Federal Virtual Training Environment
Phishing Campaign Assessment (PCA) 	A six-week engagement offered to federal and SLTT governments, critical infrastructure owners, and the private sector, the PCA evaluates an organization's susceptibility and reaction to phishing emails. PCAs provide organizations with guidance, measure effectiveness, and justify resources needed to defend against spear phishing. The assessment results provide guidance for anti-phishing training and awareness. The resulting PCA report also highlights organizational click rates for varying types of phishing emails and summarizes metrics related to user susceptibility to these attacks. **Source:** • CISA Cyber Resource Hub
Vulnerability/Cyber Hygiene Scanning 	These regular network scans focus on continuously reviewing internet-accessible systems for known vulnerabilities to help secure networks against weak configurations. Once initiated, this service is mostly automated (i.e., scans can start within 72 hours of agreement and users begin receiving reports within two weeks). As potential issues are identified, CISA notifies impacted users so they can mitigate risks prior to exploitation. The service incentivizes modern security practices and enables participants to reduce their exposure to exploitable vulnerabilities, which decreases stakeholder risk, while increasing overall resiliency. After the initial assessment, CISA will: (1) provide weekly vulnerability reports; (2) conduct enhanced scans and provide special reports on risks as they are identified; and (3) offer engineering support as needed. **Source:** • CISA Cyber Resource Hub

ADDITIONAL CYBER RESILIENCY RESOURCES

The following resources are not officially endorsed by CISA. CISA is not responsible for the validity or accuracy of any results obtained from the use of these resources.



NAME	OVERVIEW
Baldrige Cybersecurity Excellence Builder (BCEB) **Developed by:** National Institute of Standards and Technology (NIST)	The BCEB helps organizations better understand the effectiveness of their cybersecurity risk management procedures, and identity opportunities to improve their overall performance, mission, needs, and objectives. The BCEB combines concepts in the NIST Cybersecurity Framework and the Baldrige Excellence Framework. This resource is intended for use by senior leaders, chief security officers (CSO), and chief information officers (CIO) responsible for mission-driven, cybersecurity-related policy and operations. **Sources:** • Baldridge Cybersecurity Initiative • Baldridge Excellence Builder
Cybersecurity Assessment Tool (CAT) **Developed by:** Federal Financial Institutions Examination Council (FFIEC)	This diagnostic test allows organizations to determine their risk level and the maturity of their cybersecurity programs. The CAT allows management to make risk-driven security decisions across several categories (i.e., delivery channels, connection types, external threats, and organizational characteristics). The assessment consists of two parts: • The **Inherent Risk Profile** outlines the level of risk associated with specific technologies and connection types, delivery channels, online/mobile products, technology services, organizational characteristics, and external threats. • The **Cybersecurity Maturity Profile** determines whether an institution can support preparedness within areas such as cyber risk management and oversight; threat intelligence and collaboration; cybersecurity controls; external dependency management; and cyber incident management and resilience. Upon completion of both parts, management can evaluate the alignment of an institution's risk and preparedness. This tool is downloadable and can be self-administered by a public safety agency. **Source:** • FFIEC Cybersecurity Assessment Tool

NAME	OVERVIEW
Multi-State Information Sharing and Analysis Center (MS-ISAC) **Developed by:** Center for Internet Security (CIS) 	The MS-ISAC, supported by DHS, is the focal point for cyber threat prevention, protection, response and recovery for U.S. SLTT governments. Membership to the MS-ISAC is open to all U.S. SLTT government entities. Membership includes direct access to cybersecurity advisories and alerts, vulnerability assessments and incident response for entities experiencing a cyber threat; secure information sharing through the Homeland Security Information Network (HSIN) portal, tabletop exercises, a weekly malicious domains/Internet Protocol report, multiple DHS initiatives, and MS-ISAC National Webinars. Cyber security capabilities available through MS-ISAC include download of CIS controls, CIS Controls Self-Assessment Tool, CIS Risk Assessment Method, CIS CyberMarket, and Albert. **Source:** • Multi-State Information Sharing and Analysis Center
Next Generation 911 Security (NG-SEC) Audit Checklist **Developed by:** National Emergency Number Association (NENA) 	A companion to the *NENA Security for Next-Generation 911 Standard (NG-SEC) Standard* (NENA 75-001), the *NG-SEC Audit Checklist* provides a summary of the requirements detailed in the standard and is a method for documenting an NG-SEC audit. This checklist allows public safety users and auditors to record a 911 entity's compliance with the standard (e.g., acceptable use policy, authentication/password policy, data protection). Each checklist item is categorized as a requirement or best practice. **Source:** • NENA Next Generation 9-1-1 Security (NG-SEC) Audit Checklist
NIST Cybersecurity Framework **Developed by:** NIST 	The NIST Cybersecurity Framework is designed to improve the cybersecurity of critical infrastructure and complement existing risk management processes. Although it was designed specifically for critical infrastructure organizations, it is used in the operations of many other public and private sector partners (including federal agencies). The framework provides a common taxonomy for organizations to: (1) describe their current cybersecurity posture; (2) define their target state for cybersecurity; (3) identify and prioritize opportunities for improvement; (4) assess progress toward the target state; and (5) communicate among internal and external stakeholders about cybersecurity risk. When implemented in conjunction with DHS Threat and Hazard Identification and Risk Assessment (THIRA)/Stakeholder Preparedness Review (SPR) requirements, network operators can assign values to risks, measure costs, and outline the steps needed to mitigate and reduce risk. **Sources:** • NIST Cybersecurity Framework • NIST Cybersecurity Framework—Frequently Asked Questions

NAME	OVERVIEW
Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53 Rev. 5) **Developed by:** NIST 	This Special Publication covers the steps in NIST's Risk Management Framework, which address controls outlined in Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Information and Information Systems*. This includes selecting an initial set of baseline security and privacy controls based on a FIPS 199 (*Standards for Security Categorization of Federal Information and Information Systems*) worst-case impact analysis. The document offers a process for selecting controls to protect organizational operations and assets. The publication also describes how network administrators can develop specialized sets of controls and overlays, tailored for specific types of missions/business functions, technologies, or operational environments.[5] **Source:** • NIST Security and Privacy Controls for Information Systems and Organizations

NEXT STEPS

To address potential cybersecurity threats, public safety organizations should review or develop cybersecurity continuity of operations plans and consider communications operability, interoperability, resiliency, and security with respect to their own networks, as well as with third-party service/interconnection providers.

Organizations should perform regular cyber risk and resiliency assessments and use the findings to:

- **Develop** incident response plans, recovery plans, and continuity of operations plans to assist in cybersecurity incident response;
- **Exercise** plans so they can be validated, refined, and updated;
- **Incorporate** lessons learned into recovery planning processes and strategies; and
- **Train** response personnel on the latest security, resiliency, continuity, and operational practices and maintain in-service training as new technology and methods are made available.

Public safety stakeholders should continue to work with CISA to: (1) implement consistent cybersecurity standards, policies, and procedures; and (2) develop interoperability and implementation guidance for emergency communications deployments.

TO FIND OUT MORE

For more information on cybersecurity for public safety communications systems and how to conduct these assessments, contact CISA at PublicSafetyComms@cisa.dhs.gov.

[1] Presidential Policy Directive -- Critical Infrastructure Security and Resilience. February 12, 2013.
[2] CISA, "2018 SAFECOM Nationwide Survey Results – National-Level Summary," August 2018.
[3] Respondents represent public safety answering points (PSAP)/emergency communications centers (ECC) exclusively.
[4] Agencies are encouraged to implement the National Institute of Standards and Technology (NIST) Cybersecurity Framework.
[5] CISA's Interoperable Communications Technical Assistance Program (ICTAP) provides subject matter experts to guide public safety organizations through the NIST Special Publication (SP) 800-53 compliance assessment. In coordination with CISA's Cybersecurity Division and Integrated Operations Division, ICTAP provides cyber assessments for 911/PSAP/ECC dispatch and land mobile radio systems using the NIST SP 800-53 framework.