CYBERSECURITY RESOURCES FOR 9-1-1 CENTERS

Public safety communications entities, such as Emergency Communications Centers (ECCs), Public Safety Communications Centers (PSCCs), and Public Safety Answering Points (PSAPs), are a highly visible and important part of Emergency Services Sector communications, and therefore present an appealing target to cybersecurity threat actors. As the frequency and sophistication of cybersecurity incidents continues to increase, it is important for public safety communications entities to be more proactive in safeguarding their ability to continue to function and complete their mission. The Cybersecurity and Infrastructure Security Agency (CISA) assists public safety organizations to seamlessly and securely communicate during steady state and emergency operations to keep America safe, secure, and resilient. This document describes several CISA resources available to public safety communications organizations to help enhance their cybersecurity posture and resilience.

ADVISORS

Cybersecurity Advisors

The Cybersecurity Advisors (CSAs) offer cybersecurity assistance to critical infrastructure owners and operators and state, local, tribal, and territorial (SLTT) governments. CSAs introduce organizations to various CISA cybersecurity products and services. CSAs can provide cyber preparedness; assessments and protective resources; strategic messaging; working group support and leadership; partnership in public-private development; and incident coordination and support in times of cyber threat, disruption, and attack. To request assistance, contact your CISA Regional Office.

Emergency Communications Coordinators

Emergency Communications Coordinators are located across the country to engage stakeholders and address the complex issues facing the emergency communications ecosystem. For more information, contact your Emergency Communications Coordinator.

National Council of Statewide Interoperability Coordinators

National Council of Statewide Interoperability Coordinators (NCSWIC) supports Statewide Interoperability Coordinators (SWIC) by developing products and services to assist them with leveraging their relationships, professional knowledge, and experience with public safety partners involved in interoperable communications at all levels of government. For more information, contact NCSWIC.

ASSESSMENT ASSETS

Cybersecurity Assessments

Cybersecurity Infrastructure Survey

The Cyber Infrastructure Survey (CIS) evaluates the effectiveness of organizational security controls, cybersecurity preparedness, and the overall resilience of an organization's cybersecurity ecosystem across five domains – cybersecurity management, cybersecurity forces, cybersecurity controls, cyber incident response, and cyber dependencies.

Cyber Security Evaluation Tool

The Cyber Security Evaluation Tool (CSET) is a stand-alone desktop application that guides asset owners and operators through a systematic process of evaluating their existing Information Technology/Operation Technology. CSET includes the Ransomware Readiness Assessment (RRA), to help organizations better assess how well they are equipped to defend and recover from a ransomware incident.

Cyber Resilience Review

The Cyber Resilience Review (CRR) is an interview-based assessment that evaluates an organization's operational resilience and cybersecurity practices and evaluates the maturity of an organization's capacities and capabilities in performing, planning, managing, measuring, and defining cybersecurity capabilities.

External Dependency Management

The External Dependency Management (EDM) is an interview-based assessment that evaluates an organization's management of external dependencies, focusing on the relationship between an organization's high-value services and assets and evaluates how an organization manages risks derived from its use of the Information and Communications Technology Supply Chain.
For more information about cybersecurity assessments, visit the Cyber Resource Hub.

Public Safety Communications and Cyber Resiliency Toolkit

This toolkit assists 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. For information, download the Toolkit.

SYSTEMS AND PROGRAM ASSETS

Transition to Next Generation 9-1-1

NG911 Incident-Related Imagery Impacts 101

This document provides public safety and emergency communications leadership with considerations for addressing acceptance of incident-related imagery through 9-1-1 systems, such as establishing data management policies and procedures, assessing training and educational requirements, supporting staff wellness, and assessing recruitment and retention polices.

NG911 Self-Assessment Tool

This tool helps ECC and PSAP administrators and oversight personnel evaluate a system's NG9-1-1 maturity state and understand the next steps necessary to continue NG9-1-1 deployment progress.

Geographic Information System (GIS) Lifecycle Best Practices Guide

This guide provides an overview of the GIS lifecycle, best practices for each phase of the lifecycle, and resources for GIS support.

Cybersecurity for 9-1-1 and NG9-1-1 Systems

Cyber Risks to 911: TDoS

This factsheet familiarizes public safety communications partners with TDoS threats to 9-1-1.

Cyber Risks to NG911

This White Paper provides an overview of the cyber risks that will be faced by NG9-1-1 systems.

Two Things Every 911 Center Should Do To Improve Cybersecurity

This document highlights actionable steps that ECCs/PSAPs can take to enhance their cybersecurity posture.

PSAP Ransomware Poster

This poster provides comprehensive, customizable information to stakeholders on how to protect PSAPs and ECCs from ransomware. Although the poster's focus is on ransomware, its recommendations are applicable across a range of cyber threats.

For information, visit the Transition to Next Generation 911 page.

Interoperable Communications Technical Assistance Program

9-1-1/PSAP/LMR Cyber Awareness

This offering introduces public safety communications stakeholders to common cybersecurity threats and vulnerabilities affecting 9-1-1/PSAP/ECC/Land Mobile Radio (LMR) environments. Topics include ransomware attacks and their impact, TDoS attacks against administrative lines and 9-1-1, exposed networks and devices, why individual logons and password protection is critical, cryptojacking and email phishing. It also discusses basic best practices to improve the secure use of emergency communications technologies in daily operations. In addition, guidance is provided on responding to and reporting cyber incidents.

9-1-1/PSAP/LMR Cyber Assessment

The cybersecurity risk assessment technical assistance offering provides organizations with a review of their cyber posture in accordance with nationally recognized best practices guidelines.

For more information, visit the Interoperable Communications Technical Assistance Program Resources page.

National Cyber Awareness System

These advisories, alerts, analysis reports, current activities, weekly security bulletins, and tips alert readers of emerging cyber threats and vulnerabilities. View the Cybersecurity Alerts & Advisories.

CISA Incident Reporting System

This provides a secure, web-enabled means of reporting computer security incidents to CISA. This system assists analysts in providing timely handling of your security incidents as well as the ability to conduct improved analysis. For more information, visit the Incident Reporting System or email Central@cisa.dhs.gov.

Shields Up

The Shields Up webpage provides the latest cybersecurity updates and technical guidance from CISA and its critical infrastructure partners to ensure awareness of potential threats. The Shields Up webpage is updated as new information becomes available. Resources include guidance for all types of organizations, recommendations for corporate leaders and CEOs, and steps individuals can take to protect themselves. For more information, visit Shields Up.

For more information visit the CISA Emergency Services Sector webpage or email EmergencyServicesSector@cisa.dhs.gov.