ECC Cybersecurity and Incident Handling Resources

A range of resources and tools to ensure an ECC is prepared to deploy a rapid response plan to a cybersecurity incident. The resources and services can help ECC's assess their cyber resilience, improve their security posture, and respond effectively to cyber threats.

Cybersecurity Committee ECC Cybersecurity and Incident Handling Resources

Cybersecurity and Infrastructure Security Agency (Accessed May 2023)	CISA.gov is the primary source of information and navigation page for all the programs and services that CISA and DHS offer to both public and private organizations. CISA is "America's Cyber Defense Agency, and leads the national effort to understand, manage, and reduce risk to our critical infrastructure." Utilize the multiple resources and tools, reports, services, and programs to find dozens of helpful tools which can ensure your agency/ECC is prepared to deploy a rapid response plan. CISA Central contact information is central@cisa.gov and 888-282-0870
CISA Cyber Resilience Review Self Assessment (Accessed April 2023, Report released April 2020)	CISA's Cyber Resilience Review (CRR) Self-Assessment's purpose is to enable organizations to conduct a self-assessment using the CRR. It provides a measure of an organization's cyber resilience capabilities. The CRR Self-Assessment also enables an organization to assess its capabilities relative to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF).
CISA Cyber Resilience Review Supplemental Guide (Accessed April 2023, Guide released 2016)	The CISA Cyber Resilience Review Guide is a supplemental resource that assists organizations who plan to do a CRR self-assessment or have already conducted a CRR self-assessment. Any ECC interested in implementing or maturing operational resilience capabilities for critical services will find this resource useful.
SANS Internet Stormcast Podcast (Free) (Accessed April 2023)	The SANS institute sponsors an Internet Stormcast which is a daily 5-minute podcast outlining any information on vulnerabilities that are out, patches that need to be done, and other newsworthy cybersecurity information.

Cybersecurity Committee ECC Cybersecurity and Incident Handling Resources

APCO Cybersecurity Fundamentals for the ECC APCO Intermediate Cybersecurity Principles for the ECC (Accessed June 2023)	The APCO Cybersecurity Fundamentals for the ECC course is built on the experiences of public safety cybersecurity experts and ECC professionals. This course will provide ECC professionals with foundational knowledge of cyberattacks, including the anatomy of a cyberattack, signs of an ongoing cyberattack and mitigation techniques. This includes preparing for cyberattacks, response to those attacks and the type of data to protect for post-attack forensics. The APCO Intermediate Cybersecurity Principles for the ECC course is designed for Public Safety Information Technology (IT) personnel, IT Leadership personnel who work on critical networks within ECCs and ECC supervisory staff charged with IT and Cybersecurity responsibilities. This course will provide an understanding of a hacker's perspective, motives, and weaknesses. It includes additional information on incident response by looking at the conditions that contribute to a network's vulnerability and dissecting the step-by-step process of a cyber-attack. This process includes mitigation planning by learning to recognize an attack and stop the exploitation before it spreads. This course also covers recovery, and some forensics by learning what countermeasures can be taken before and during an attack to prevent further spread.
NIST Computer Security Incident Handling Guide (Accessed April 2023, Guide released 2012)	The National Institute of Standards and Technology (NIST) Computer Security Incident Handling Guide is a documented incident response process that features ongoing learning and advancements to assist on how to best protect an ECC. The four stages are: Preparation, Detection/Analysis, Containment/Eradication, and Recovery.
NIST-CSRC Publications (Accessed May 2023)	The National Institute of Standards and Technology Computer Security Resource Center (NIST-CSRC) is an extensive collection of standards, guidelines, recommendations, and research on the security and privacy of information and information systems.

Cybersecurity Committee ECC Cybersecurity and Incident Handling Resources

Homeland Security Cyber Infrastructure Survey Tool (C-IST) (Accessed May 2023)	The Homeland Security Cyber Infrastructure Survey Tool (C-IST) is a free assessment of essential cybersecurity practices in-place for critical services within critical infrastructure organizations. This tool is a structured assessment of over 80 cybersecurity controls grouped under five key surveyed topics. After the assessment the Department of Homeland Security will provide a user-friendly dashboard that the ECC can review and interact with the surveyed findings. These services are no cost but are limited.
CISA Vulnerability Scanning (VS) (Accessed May 2023)	CISA's Vulnerability Scanning (VS) is a persistent "internet scanning-as-a-service" and part of CISA's service offerings. The VS service includes Target Discovery and Vulnerability Scanning. There are four phases, which include the participation of CISA and the ECC, in this service: Pre-Planning, Planning, Execution and Post-Execution. These services are no cost but are limited.
FCC Task Force on Optimal PSAP Architecture (TFOPA) (Accessed April 2023)	The FCC Task Force on Optimal PSAP Architecture looks at Next Generation 9-1-1 (NG9-1-1) cost, cybersecurity, and funding sustainment model. The FCC TFOPA reports provide checklists specific to public safety communications that ECCs can use before, during, and after a cyberattack.
CISA Resource Hub (Accessed May 2023)	The CISA Resource Hub is a comprehensive list of CISA's cybersecurity assessments that evaluate operational resilience, cybersecurity practices, organizational management of external dependencies, and other key elements of a robust and resilient cyber framework. These professional and no-cost assessments are provided upon request on a voluntary basis and can help any ECC with managing risk and strengthening the cybersecurity of our Nation's critical infrastructure.

Cybersecurity Committee ECC Cybersecurity and Incident Handling Resources

CISA Risk and Vulnerability Assessments (Accessed May 2023)	ECC's can schedule a Risk and Vulnerability Assessment (RVA) through the Cybersecurity and Infrastructure Security Agency. CISA then takes the data from these RVAs that are conducted and provide an analysis sample of attack vectors a threat actor could take to compromise a network. These attack vectors and vulnerabilities are representative of those CISA observed in risk and vulnerabilities assessments performed in the fiscal year. The RVA analysis is then then mapped to the MITRE ATT&CK® framework in an infographic. Examples: 2021 FY RVAs Analysis 2021 FY RVAs Mapped to the MITRE ATT&CK® Framework Infographic