Homeland Security

Emergency Services Sector Cybersecurity Initiative

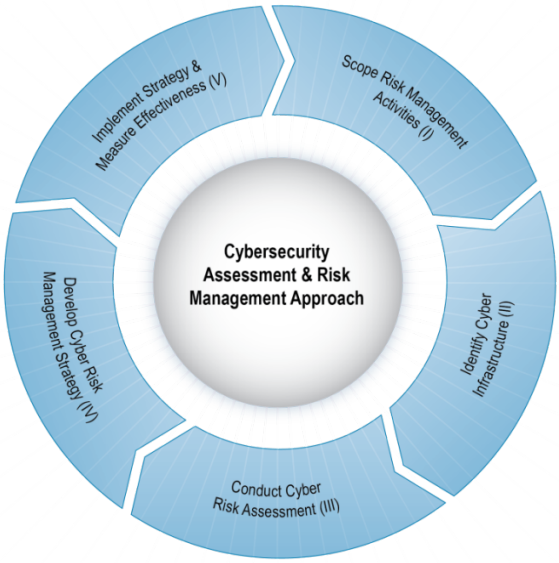
The *Emergency Services Sector Cybersecurity Initiative* is an ongoing effort to enable the Emergency Services Sector (ESS) to better understand and manage cyber risks and to coordinate the sharing of cyber information and tools between subject matter experts (both inside and outside the federal government) and the ESS disciplines.

Emergency Services Sector Cyber Risk Assessment

In 2012, the *Emergency Services Sector Cyber Risk Assessment* (ESS CRA) was developed using the Department of Homeland Security's Cybersecurity Assessment and Risk Management Approach (CARMA) methodology. The *ESS CRA* is the first ESS-wide cyber risk assessment that identifies and analyzes strategic cyber risks to ESS infrastructure. The *ESS CRA* can help sector stakeholders understand and manage cyber threats, vulnerabilities, and consequences in a collaborative, prioritized manner, and provides a national-level risk profile that ESS stakeholders can use to prioritize how they spend resources and where to focus training, education, equipment investments, grant requests, and further study.

Emergency Services Sector Roadmap to Secure Voice and Data Systems

In 2014, the *Emergency Services Sector Roadmap to Secure Voice and Data Systems* (Roadmap) was developed as a follow-up to the *ESS CRA*. The Roadmap identifies and discusses multiple measures to address the risks identified in the ESS CRA. The measures are intended to address cyber risks either by reducing the likelihood that a risk could be realized, by reducing the consequences of a cyber incident if it were to occur, or both. The Roadmap discusses each measure and includes justification for the response, sector context, barriers to implementation, and suggestions for implementation.



Cybersecurity Assessment & risk Management Approach
CARMA
(Courtesy of DHS)

Enhanced Cybersecurity Services for the Emergency Services Sector

Enhanced Cybersecurity Services (ECS) is a voluntary, information-sharing program that helps the ESS improve protection of its systems from unauthorized access, exploitation, or data exfiltration, and helps protect against cyber threats that could otherwise harm their systems. ECS consists of the operational processes and security oversight required for the Federal Government to share sensitive and classified cyber threat information with Commercial Service Providers, who will be able to protect themselves and their critical infrastructure customers, and with Operational Implementers, who are critical infrastructure entities who wish to protect themselves from these threats.

Cyber Resilience Review

The Cyber Security Evaluation Program conducts no cost, voluntary Cyber Resilience Reviews (CRR) to evaluate and enhance cybersecurity capacities and capabilities within all 16 critical infrastructure sectors, as well as state, local, tribal, and territorial governments. The CRR seeks to understand cybersecurity critical for an organization's success by focusing on protection and sustainment practices within ten key domains that contribute to the overall cyber resilience of an organization.

Executive Order 13636 Improving Critical Infrastructure Cybersecurity
Presidential Policy Directive-21 Critical Infrastructure Security and Resilience

Facing threats to our nation from cyber-attacks that could disrupt our power, water, communications, and other critical infrastructure, the President issued Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive (PPD)-21 Critical Infrastructure Security and Resilience. These policies reinforce the need for holistic thinking about security and risk management. Implementation of the EO and PPD will drive action toward system and network security and resiliency, while simultaneously enhancing the efficiency and effectiveness of the U.S. government's efforts to secure critical infrastructure and make it more resilient.

For more information on any of these, visit the Emergency Services Sector Cybersecurity Initiative at http://www.dhs.gov/emergency-services-sector-cybersecurity-initiative, or email the Emergency Services Section at essteam@hq.dhs.gov.

OMB Control Number: 1601-0014
Expiration Date: 10/31/2017

Stakeholder Feedback Form

General Information

Please select the category that best describes your organization: Select one

Overall Assessment

1. Please evaluate the following statement: The information received through this activity or product was current and relevant.

Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree

2. Please provide any recommendations that you may have on how future activities or products of this type could be improved to enhance their relevance.

3. Please evaluate the following statement: The information received through this activity or product will effectively inform my decision making regarding safety and security risk mitigation and resilience enhancements.

Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree

4. Please provide any recommendations that you may have on how future activities or products of this type could be improved to increase their value in support of your mission.

5. Please evaluate the following statement: I will encourage my agency/organization to incorporate information I learned through this activity or product into our safety, security, or resilience practices.

Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree

6. Please provide any recommendations that you may have on how future activities or products of this type could be improved so they can be better incorporated into safety, security, or resilience practices across the critical infrastructure community.

Submit to: essteam@hq.dhs.gov

Privacy Notice

Paperwork Reduction Act Burden Notice