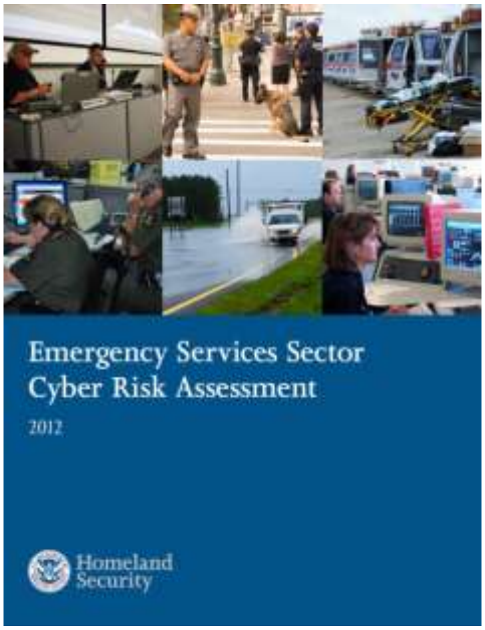
Homeland Security

Emergency Services Sector Cyber Risk Assessment



The Emergency Services Sector (ESS) is a system of preparedness, response, and recovery elements that form the Nation's first line of defense for preventing and mitigating risks from manmade and natural threats. ESS is a primary "protector" for other critical infrastructure sectors. Over the past decade, ESS has become increasingly dependent on a variety of cyber-related assets, systems, and disciplines to carry out its missions. In addition to the cyber risks presented by natural hazards—such as catastrophic weather or seismic events—ESS also faces threats from criminals, hackers, terrorists, and nation-states, all of whom have demonstrated varying degrees of capability and intention to attack ESS cyber infrastructure.

In 2011, through the Critical Infrastructure Partnership Advisory Council framework, ESS began the sector-wide 2012 ESS Cyber Risk Assessment (ESS-CRA) using the Department of Homeland Security National Cyber Security Division's Cybersecurity Assessment and Risk Management Approach (CARMA) methodology. The 2012 ESS-CRA is the first ESS-wide cyber risk assessment that analyzes strategic cyber risks to ESS infrastructure. The assessment results will help the sector understand and manage cyber threats, vulnerabilities, and consequences in a collaborative, prioritized manner. Practitioners who address the CRA's results will no doubt be better prepared to handle cyber incidents, and thus, better prepared to continue serving their communities and the nation at large. Ultimately, the ESS-CRA process provides a national-level risk profile that ESS partners can use to prioritize how they spend resources and where to focus training, education, equipment investments, grant requests, and further study.

Cyber Risk Management Process

Risk assessment participants from state and local governments, as well as the private sector, represented all six sector disciplines: Law Enforcement, Fire and Emergency Services, Emergency Medical Services, Emergency Management, Public Works, and Public Safety Communications and Coordination/Fusion. The CARMA process steps were:

1. First, the assessment team was established, with key leaders and ESS SMEs.
2. ESS-CRA participants then conducted the initial scoping of the assessment. During this process, the ESS-CRA participants concluded that the ESS-CRA engagement should be a sector-wide effort, rather than focusing on individual public safety disciplines, and should be used to address high profile cyber threats.
3. With initial scoping complete, the participants began the process of defining and developing a draft set of disciplines for the ESS-CRA.

The risk assessment consisted of seven evaluation sessions to solicit input from ESS subject-matter experts. The sessions covered seven scenarios, including:

1. Natural Disaster Causes Loss of 9-1-1 Capabilities
2. Lack of Availability of Sector Database Causes Disruption of Mission Capability
3. Compromised Sector Database Causes Corruption or Loss of Confidentiality of Critical Information
4. Public Alerting and Warning System Disseminates Inaccurate Information
5. Loss of Communications Lines Results in Disrupted Communications Capabilities
6. Closed-Circuit Television Jamming/Blocking Results in Disrupted Surveillance Capabilities
7. Overloaded Communications Network Results in Denial of Service Conditions for Public Safety and Emergency Services Communications Networks.

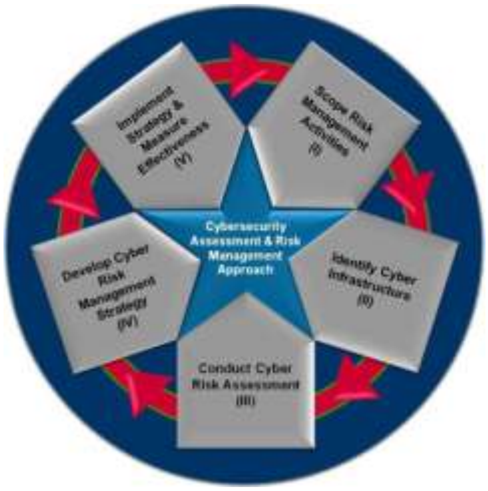
> *The ESS-CRA process provides a national-level risk profile that ESS partners can use to prioritize how they spend resources and where to focus training, education, equipment investments, grant requests, and further study.*

Each scenario evaluated threats, vulnerabilities, and consequences to ESS cyber infrastructure. Stakeholders chose scenarios based on what would have the widest impact; the scenarios likely to affect the most disciplines at a time.

The final ESS-CRA report includes a risk profile showing how the scenarios would affect each discipline, including the operational impact. Cyber risks to each discipline are ranked from high to low in terms of likelihood and consequence. The assessment approach is not intended to be guidance for individual entities' risk management activities. Instead, by increasing the awareness of risks across the public and private sector domains, the ESS-CRA serves as a foundation for ongoing national-level collaboration to enhance the security and resilience of the ESS disciplines.

Next Steps in the Process

The ESS-CRA is an initial effort to assess cyber risks of national concern across all six ESS disciplines based on the knowledge and expertise of sector subject matter experts, and it is the beginning of a comprehensive ESS cyber risk management initiative. Following the ESS-CRA, the next phase in the CARMA lifecycle is to determine how the identified risks should be addressed. This will be accomplished via the *Emergency Services Sector Cybersecurity Roadmap*, which will outline the sector's risk management strategies.


Implement Strategy & Measure Effectiveness (V)
Scope Risk Management Activities (I)
Cybersecurity Assessment & Risk Management Approach
Develop Cyber Risk Management Strategy (IV)
Identify Cyber Infrastructure (II)
Conduct Cyber Risk Assessment (III)

CARMA provides a repeatable framework for ESS to identify and prioritize cyber risks of concern to infrastructure that supports mission essential functions across the ESS disciplines. CARMA's five-stage process encompasses the full risk management cycle.

Contact Information

If you have any further questions about the ESS Cyber Risk Assessment, please send an email to ESSTeam@hq.dhs.gov.