



# INTRODUCTION TO THE EMERGENCY SERVICES SECTOR RISK MANAGEMENT AGENCY

The Emergency Services Sector (ESS) is a community of millions of highly skilled, trained personnel, along with the physical and cyber resources, that provide a wide range of prevention, preparedness, response, and recovery services during both day-to-day operations and incident response. The ESS includes geographically distributed facilities and equipment in both paid and volunteer capacities organized primarily at the federal, state, local, tribal, and territorial levels of government, such as city police departments and fire stations, county sheriff's offices, Department of Defense police and fire departments, and town public works departments. The ESS also includes private sector resources, such as industrial fire departments, private security organizations, and private emergency medical services providers. The Cybersecurity and Infrastructure Security Agency (CISA) serves as the Sector Risk Management Agency (SRMA) for this sector.

## EMERGENCY SERVICES SECTOR COLLABORATION, RESOURCES, AND TRAINING

CISA offers many resources and training materials to help manage risks, improve security, and aid the implementation and execution of protective measures across this sector. This fact sheet lists a sampling of sector collaboration mechanisms, resources, and training materials. Unless otherwise noted below, additional information can be found on the CISA website at [cisa.gov/emergency-services-sector](https://cisa.gov/emergency-services-sector).

**Collaboration**

**Emergency Services Sector Government Council (GCC), Sector Coordinating Council (SCC), and Working Groups** convene regularly; share information; and develop tools, guidelines, and products. These groups work closely to plan, implement, and execute sector-wide resilience and security programs within the Emergency Services Sector.

**Protective Security Advisors** are security subject matter experts who assist local efforts to protect critical assets and provide a local perspective to the national risk landscape. Learn more at [cisa.gov/protective-security-advisors](https://cisa.gov/protective-security-advisors).

**Cybersecurity Advisors (CSAs)** bring together critical infrastructure owner/operators with federal, state, local, and other stakeholders to maximize collaboration and minimize risk on matters of homeland security or emergency management.

**Fusion Centers** operate as state and major urban area focal points for the receipt, analysis, gathering, and sharing of threat-related information between federal; state, local, tribal, territorial (SLTT); and private sector partners. Learn more at [dhs.gov/fusion-centers](https://dhs.gov/fusion-centers).

**Homeland Security Information Network-Emergency Services (HSIN-ES)** is the trusted network for homeland security mission operations to share sensitive but unclassified (SBU) and law enforcement sensitive (LES) information. Learn more at [dhs.gov/homeland-security-information-network-hsin](https://dhs.gov/homeland-security-information-network-hsin).

**Resources**

**Emergency Services Sector Cybersecurity Framework Implementation Guidance** provides a common language that Emergency Services Sector organizations can use to assess and manage their cybersecurity risks, and uses the National Institute of Standards and Technology (NIST) voluntary Framework for Improving Critical Infrastructure Cybersecurity.

**Crisis Event Response and Recovery Access (CERRA) Framework** focuses on supporting state, local, and regional efforts to enable the successful transit and access of critical response and recovery resources before, during, and after emergencies.

**Emergency Services Sector Continuity Planning Suite (ESS-CPS)** provides a centralized collection of existing guidance, processes, products, tools, and best practices to support the development and maturation of continuity planning for the first responder community. First responders can use this resource to evaluate and improve their continuity capability and enhance their preparedness for emergencies. Learn more at [cisa.gov/emergency-services-sector-continuity-planning-suite](https://cisa.gov/emergency-services-sector-continuity-planning-suite).

**Additional ESS Resources** are located at [cisa.gov/emergency-services-sector-resources](https://cisa.gov/emergency-services-sector-resources).

**Training**

**CISA hosts the Emergency Services Sector Active Shooter Workshop** to enhance awareness of and response to an active shooter event by educating participants, describing common behaviors, and fostering communications between infrastructure owners and operators and local emergency response teams. Learn more at [cisa.gov/emergency-services-sector-active-shooter-workshop](https://cisa.gov/emergency-services-sector-active-shooter-workshop).




**The Office for Bombing Prevention (OBP)** offers free online and in-person Counter-Improvised Explosive Device (IED) training courses and awareness products to reduce risk to the Nation's critical infrastructure and enhance awareness of terrorist threats. Learn more at [cisa.gov/bombing-prevention-training](https://cisa.gov/bombing-prevention-training).

**Additional ESS Training** information is located at [cisa.gov/emergency-services-sector-training](https://cisa.gov/emergency-services-sector-training).

## SECTOR PROFILE

The Emergency Services Sector supports the other critical infrastructure sectors and assists a range of organizations and communities in maintaining public safety, security, and confidence in the government. Five disciplines—primarily performed at the state, local, tribal, and territorial level—define the operations and functions of this important sector: **Law Enforcement, Fire and Rescue Services, Emergency Medical Services, Emergency Management, and Public Works.**

### Sector Components

Human	Physical	Cyber
		
<p><b>More than 4.6 million career and volunteer professionals in five disciplines:</b></p> <ul style="list-style-type: none"> <li>• Law Enforcement</li> <li>• Emergency Management</li> <li>• Fire and Rescue Services</li> <li>• Emergency Medical Services</li> <li>• Public Works</li> </ul>	<p><b>Facilities</b> for daily operations, support, training, or storage.</p> <p><b>Equipment</b> specialized for discipline and capability (e.g., personal protective, communications, surveillance).</p> <p><b>Vehicles</b> specialized for discipline and capability (e.g., ambulances, HAZMAT, aircraft, and watercraft).</p>	<p><b>Virtual Operations</b> – Emergency operations, communications, database management, biometric activities, and security systems.</p> <p><b>Internet</b> – The Internet is widely used by the Sector to provide information and distribute alerts, warnings, and threats.</p> <p><b>Information Networks</b> – Computer-aided dispatch and watch and warning systems, information-sharing portals, and social networking are leveraged to keep the ESS informed and connected.</p>

## CRITICAL INFRASTRUCTURE SECURITY CONSIDERATIONS

- **Cyberattacks:** The Emergency Services Sector has become increasingly dependent on cyber-based infrastructure and operations, including emergency operations communications, data management, and electronic security systems. Because of this reliance, cyber infrastructure across this sector may be a key target for cyberattacks.
- **Violent Extremist and Terrorist Attacks:** Violent extremists are increasingly targeting emergency services personnel (especially law enforcement) along with public venues and crowded places. Secondary explosive devices, which aim to harm the first responders to an initial incident, pose a specific threat to this sector.
- **Chemical, Biological, Radiological (CBR) Incidents:** CBR incidents can spread across multiple jurisdictions, strain resources, and affect the health and safety of large numbers of the public and responders.
- **Natural Disasters and Extreme Weather:** More extreme weather increases the geographic magnitude and severity of disasters, requiring a surge of resources, often for extended periods, while also straining resources in partnering regions that might otherwise supply mutual aid.

## FOR MORE INFORMATION ON THE EMERGENCY SERVICES SECTOR

Contact the Emergency Services Sector Management Team at [EmergencyServicesSector@cisa.dhs.gov](mailto:EmergencyServicesSector@cisa.dhs.gov) or learn more at [cisa.gov/emergency-services-sector](https://cisa.gov/emergency-services-sector). For additional information about the Emergency Services Sector, view the Emergency Services Sector-Specific Plan at [cisa.gov/publication/nipp-ssp-emergency-services-2015](https://cisa.gov/publication/nipp-ssp-emergency-services-2015).