Emergency Services Sector-Specific Plan

An Annex to the NIPP 2013

2015

Homeland Security

TABLE OF CONTENTS

COORDINATION LETTER FROM COUNCIL CHAIRS

The Emergency Services (ES) Sector-Specific Plan (SSP) is designed to guide and integrate the sector's voluntary, collaborative efforts to improve its security and resilience over the next four years. It describes how the Emergency Services Sector (ESS) manages risks and contributes to national critical infrastructure security and resilience, as set forth in Presidential Policy Directive 21: Critical Infrastructure Security and Resilience. As an annex to the *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (NIPP 2013), this Sector-Specific Plan (SSP) tailors the strategic guidance provided in the NIPP 2013 to the unique operating conditions and risk landscape of the ESS. The sector strategy is closely aligned with the NIPP 2013 national strategy, the 2014 Joint National Priorities for Critical Infrastructure Security and Resilience, and Executive Order (EO) 13636: Improving Critical Infrastructure Cybersecurity.

This 2015 release of the ES SSP substantially updates the original plan issued in 2007 and the update issued in 2010. It represents a collaborative effort between the private sector; State, local, tribal, and territorial governments; nongovernmental organizations; and the Federal Government. This collaboration will help prioritize security and resilience initiatives and investments within and across sectors to ensure that resources are applied where they contribute the most to risk mitigation by reducing vulnerabilities, deterring threats, and minimizing the consequences of attacks and other incidents. This SSP answers NIPP 2013 Call to Action #2, which calls upon each sector to update its SSP every four years to reflect joint priorities, address sector reliance on lifeline functions, describe national preparedness efforts, outline cybersecurity efforts, and develop metrics to measure progress.

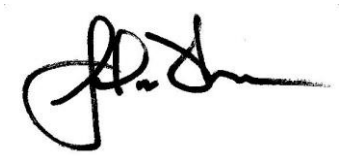
The ESS goals, priorities, and activities in this SSP were jointly determined by the Emergency Services Sector Coordinating Council (SCC) and Government Coordinating Council (GCC) and reflect the overall strategic direction for the sector. The ESS is complex with a unique mission to serve and protect the other 15 critical infrastructure sectors. The SCC believes that "protecting the protectors" is vital and is dedicated to working with the sector partnership community to ensure the security and resilience of its infrastructure and, first and foremost, its personnel. The GCC is also committed to this effort and will collaborate with its sector partners to implement and support security and resilience programs for the ESS consistent with the NIPP 2013 and this SSP.

This SSP also reflects the maturation of the ESS partnership and the progress made by the sector since the 2010 SSP to address its evolving risk, operating, and policy environments. Major sector accomplishments since 2010:

- Developed two documents—*Emergency Services Sector-Cyber Risk Assessment* in 2012 and *Emergency Services Sector Roadmap to Secure Voice and Data Systems* in 2014—to establish baseline national-level cyber risk and identify risk mitigation strategies.
- Developed an ESS self-assessment tool in 2010, intended to assist ESS organizations in assessing their current capabilities, enhancing information sharing, reducing risk, and increasing resilience through the establishment of a capabilities database and Sector Risk Profile. The ES Sector-Specific Agency (SSA), in coordination with the ES SCC, is working to incorporate the functions of this tool into the IP Gateway.
- Contributed vital input to Project Responder 3 and Project Responder 4 studies in 2012 and 2014 to identify and prioritize sector capabilities and needs.
- Formed the Credentialing and Disaster Reentry Working Group in 2012 to support the development of a standardized, cross-jurisdictional approach to crisis reentry for public and private emergency responders.
- Developed and conducted the Twisted Fate exercise in 2012 for first-responder chief officers and senior officials, focusing specifically on ESS resilience and continuity of operations.
- Formed a Working Group on Medical Countermeasures in 2011 to support the development of national strategy protecting the health of emergency services personnel regarding major public health incidents such as pandemics.
- Acquired information on new medical treatments to help with the safety and resilience of sector personnel during an ESS response to biological incidents, courtesy of ESS professionals from the Emergency Services Coalition for Medical Preparedness.

These achievements, which represent the effective collaboration of the SCC, GCC, and the Emergency Services Sector-Specific Agency, clearly demonstrate the sector's progress in working toward a rational approach to develop, prioritize, and implement effective security programs and resilience strategies.

In the same shared purpose that guided these actions and their support for the framework, concepts, and processes outlined in the NIPP 2013 and EO 13636, ESS partners look forward to continuing their efforts to enhance the security and resilience of the Nation's critical infrastructure assets.



John Thompson
Deputy Executive Director and COO,
National Sheriffs' Association;
Chair, Emergency Services
Sector Coordinating Council

Caitlin A. Durkovich
Assistant Secretary
Office of Infrastructure Protection
U.S. Department of Homeland Security;
Chair, Emergency Services Sector
Government Coordinating Council

EXECUTIVE SUMMARY

The Emergency Services Sector (ESS) includes a diverse array of disciplines and capabilities that enables a wide range of prevention, preparedness, response, and recovery services to serve and protect the Nation's critical infrastructure as well as the American public. As its operations provide the first line of defense for nearly all critical infrastructure sectors, a failure or disruption in the ESS could result in significant harm or loss of life, major public health issues, long term economic loss, and cascading disruptions to other critical infrastructure.

Emergency Services Sector Assets and Risks

The majority of ESS operations are organized, staffed, and managed at the State, local, tribal, and territorial (SLTT) level and are therefore highly geographically distributed. The sector's personnel—encompassing law enforcement, fire and rescue services, emergency medical services, emergency management, and public works disciplines—are its most critical assets. With the mission to prepare for and respond to a wide variety of emergencies, the ESS is vulnerable to the same risks those emergencies present to other critical infrastructure. The sector's diversity in organization, mission, and assets makes disabling the entire emergency services system difficult. However, damage or disruption to ESS components can dramatically impede the protection of the public, other critical infrastructure sectors, and disciplines internal to the sector.

Given the critical mission of the ESS, risks to its operations and functions could prove disastrous to the safety and morale of the public, the protection of other critical infrastructure sectors, and the safety of its own disciplines. Significant risks to the sector derive from cyberattacks or disruptions; natural disasters and extreme weather; violent extremist and terrorist attacks; and chemical, biological, radiological, and nuclear incidents.

Partnering to Improve Security and Resilience

Emergency incidents often affect multiple jurisdictions at different levels, necessitating prevention, preparedness, response, and recovery coordination among Federal, State, local, tribal, territorial, private sector, or other nongovernmental critical infrastructure partners. ESS personnel are intricately involved in such coordination; employ a robust risk management framework to improve understanding of threats, vulnerabilities, and consequences; and provide sector partners with tools, guidelines, information, best practices, and resources to facilitate more effective risk assessments and risk management decisions.

The NIPP 2013 partnership structure enables ESS personnel to collaborate (on a voluntary basis) directly with their peers through the Sector Coordinating Council (SCC) and with Federal, regional, and local partners through the Government Coordinating Council (GCC). Through this partnership, the ESS has developed tools, resources, and programs that support sector-wide risk management and maximize partners' limited resources. Key examples include a sector-wide cyber risk assessment methodology and roadmap, as well as tabletop exercises and strategic workshops focused on first responder credentialing and disaster re-entry, continuity of ESS operations, and sector research and development needs and priorities.

2015 Sector-Specific Plan

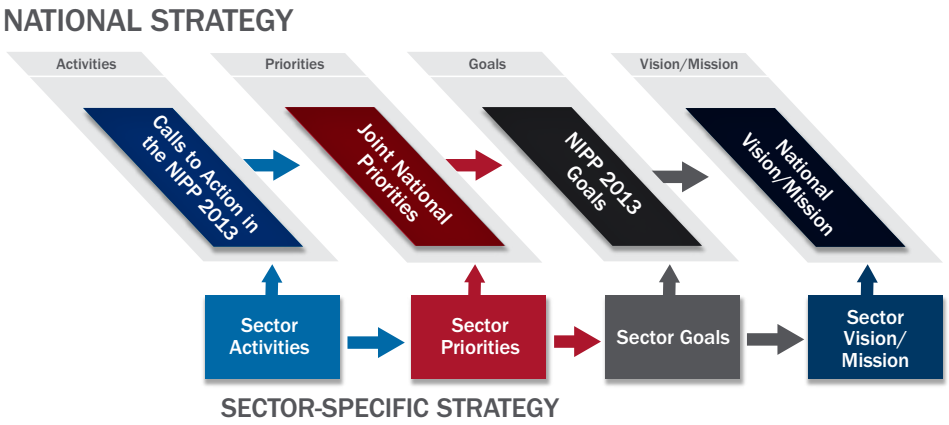
As part of this 2015 Sector-Specific Plan, the Emergency Services SCC and GCC have identified goals and priorities to guide the sector's security and resilience efforts over the next four years. The four goals are:

- **Partnership Engagement**—Continuous growth and improvement of sector partnerships, which enable the sector to effectively sustain collaborative dialogues to address risk mitigation and resilience efforts within the sector.
- **Situational Awareness**—Support an information-sharing environment that ensures the availability and flow of accurate, timely, and relevant sector information, intelligence, and incident reporting.
- **Prevention, Preparedness, and Protection**—Employ a risk-based approach to improve the preparedness and resilience of the sector's overall capacity to perform its mission through targeted decisions and initiatives.
- **Recovery and Reconstitution**—Improve the operational capacity, sustainability, and resilience of the sector and increase the speed and efficiency of restoration of normal services and activity following an incident.

To achieve these goals, sector partners developed 12 priorities to focus their efforts. The priorities include developing and utilizing processes and mechanisms to support sector partnerships and information sharing, sharing sector-specific best

practices, and enabling sector partners to implement their missions. In addition, the councils identified 18 activities that sector partners plan to collaboratively conduct, as resources allow, to improve the security and resilience of emergency services in the United States. Predominant themes include an increased focus on technological solutions and cybersecurity, a renewed drive for cross-discipline and cross-sector collaboration, and defining current sector risk assessment and information-sharing capabilities and requirements.

Figure ES-1: Alignment of National and Sector-Specific Goals, Priorities, and Activities



As a result, progress toward sector goals, priorities, and activities contributes directly to national achievements under the NIPP 2013. Appendix B demonstrates the detailed alignment of the Sector-Specific Plan to NIPP 2013 goals, the Joint National Priorities for Critical Infrastructure Security and Resilience, and the NIPP 2013 Calls to Action.

1 INTRODUCTION

This 2015 Emergency Services (ES) Sector-Specific Plan (SSP) is designed to guide voluntary, collaborative efforts to improve the sector's security and resilience over the next four years. It describes how the Emergency Services Sector (ESS) manages risks and contributes to national critical infrastructure security and resilience, as set forth in Presidential Policy Directive 21: Critical Infrastructure Security and Resilience. As an annex to the NIPP 2013, this SSP tailors the strategic guidance and risk management framework in the NIPP 2013 to the unique operating conditions and risk landscape of the ESS.

Most importantly, this SSP sets the strategic direction for ESS security and resilience efforts by identifying shared goals, priorities, and activities for sector partners. Jointly developed by representatives of the Emergency Services Sector Coordinating Council (SCC) and Government Coordinating Council (GCC), this SSP identifies a collaborative approach to mitigate sector risks and maximize limited public-private resources. This SSP does not alter or impede the ability of ESS partners to perform their respective responsibilities under the law.

SSP development answers NIPP 2013 Call to Action #2, which requires each critical infrastructure sector to update its SSP every four years to reflect joint priorities, address sector reliance on lifeline functions, describe national preparedness efforts, outline cybersecurity efforts, and develop metrics to measure progress. The 2015 ESS goals and priorities align closely with the national goals for critical infrastructure security and resilience in the NIPP 2013 and the associated Joint National Priorities for Critical Infrastructure Security and Resilience developed in 2014 by the U.S. Department of Homeland Security (DHS). Priorities also support the implementation of Executive Orders (EOs), such as EO 13636: Improving Critical Infrastructure Cybersecurity and EO 13650: Improving Chemical Facility Safety and Security.

This ES SSP includes the following elements:

- **Chapter 2: Sector Overview**—Provides a concise description of the sector's major components, risk profile, and key public and private sector partners.
- **Chapter 3: Risk Management and National Preparedness**—Describes the sector's mechanisms to achieve its goals, specifically the sector's risk management approach, including collaborative programs, activities, and resources; its approaches to cybersecurity; sector-specific research and development (R&D) priorities; and ways in which the sector supports national preparedness for emergency incidents.
- **Chapter 4: Vision, Mission, Goals, and Priorities**—Presents the sector's vision for security and resilience, mission to enact that vision, and updated goals and priorities to support the NIPP 2013 goals, Calls to Action, and Joint National Priorities. Lists the specific activities the ES SCC and GCC plan to undertake in partnership to address sector priorities.
- **Chapter 5: Measuring Effectiveness**—Describes the planned approach the sector will use to measure the effectiveness of individual activities.
- **Appendices**—Provide additional detail to support the major chapters of this SSP.

This SSP is a living document, updated regularly to reflect changes in national policy and plans, sector composition and structure, and priorities of sector stakeholders.

Evolving Threats and Capabilities

The changing and oftentimes unpredictable nature of both manmade and natural threats is an ever-evolving challenge for response efforts. Serving and protecting the public requires ESS personnel to maintain a high level of threat awareness and associated degrees of response, as well as the capacity to respond to an increasing number of complex challenges. Evolving threats include asymmetrical attack incidents, such as active shooter and improvised explosive device (IED) incidents; biological agents and infectious diseases occurrences, such as ebola, smallpox, and tuberculosis; chemical hazard emergencies; cyberattacks; and extreme weather events. The response effort can become more challenging when these hazards are operationalized with malicious intent ("weaponized"), such as intentionally setting wildfires or releasing harmful biological or chemical agents. ESS personnel perpetually face the challenge of sustaining response levels to existing threats together with responding to evolving threats requiring new or expanded ESS capabilities. Since the 2010 SSP, the ESS

has developed additional capabilities to combat evolving threats, such as forming a Pandemic Working Group in 2013 and collaborating with DHS Science and Technology (S&T) Directorate through the First Responders Group (FRG), to ensure that critical capability gaps are prioritized in an environment of less robust resources.

Sector Objectives, Activities, and Metrics

The ESS continually reevaluates its goals and most recently released an updated set of 4 goals with 12 associated objectives in 2013. Following the release of the NIPP 2013, the ESS further reevaluated its objectives, activities, and metrics to measure progress and success. The revised objectives (equivalent to priorities for SSP development), activities, and metrics included in the 2015 ES SSP guide sector security and resilience efforts, inform decision-making, and reflect actionable activities that partners can pursue to reduce critical infrastructure risks and to improve risk management practices, taking into consideration the unique risk management perspectives and resource constraints of the sector. Implementation of this SSP also reflects how the ESS will accomplish the NIPP 2013 goals, Calls to Action, and Joint National Priorities. While the sector's goals have not drastically changed, the focus of its objectives and activities to implement those goals highlights the sector's evolving risk profile, capabilities, and needs. Predominant themes include an increased focus on technological solutions and cybersecurity, a renewed drive for cross-discipline and cross-sector collaboration, and definitions of current sector risk assessment and information-sharing capabilities and requirements.

2 SECTOR OVERVIEW

2.1 Sector Profile

The ESS is a community of millions of trained personnel along with the physical and cyber resources that enable them to provide a wide range of prevention, preparedness, response, and recovery services during both steady-state and incident management operations. The ESS includes geographically distributed facilities and equipment and highly skilled personnel that provide services in both paid and volunteer capacities. The sector is organized primarily at the Federal, State, local, tribal, and territorial (SLTT) levels of government, such as city police departments, 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 (EMS) providers.

As the ESS focuses on protecting other sectors and the public, unique challenges arise in addressing the security and resilience of the ESS as critical infrastructure. The incapacitation of any of the assets, networks, or systems in this sector, whether physical or virtual, could cause significant harm or loss of life, public health issues, and/or long-term economic loss.

This Sector Profile provides an overview of ESS assets, components, disciplines, and capabilities, and the key characteristics of each that influence security and resilience in the sector.

Key Sector Operating Characteristics

The ESS is the most geographically distributed sector with more than 2.5 million personnel serving every location in all 50 States, five territories, and the District of Columbia.
Security and resilience planning and decisions take place primarily at the regional and local level. Complex systems and dispersed assets make it difficult to disable the entire system, but also pose challenges to coordination across disciplines, regions, and levels of government.

First response can greatly affect the resulting severity and duration of emergency events.
ESS operations provide the first line of defense for nearly all critical infrastructure sectors and the American public during natural disasters and other physical emergencies. Response decisions and operations can determine how quickly other critical services are restored. Effective preparedness requires regional and local ESS coordination with every other critical service.

Adaptability and flexibility are hallmarks of ESS operations.
Emergency services are required and expected for a vast array of incidents, and responders may be exposed to unfamiliar situations for which they have not trained, particularly first-of-a-kind disasters. ESS personnel are therefore experts in adapting to emergency situations. Flexibility and adaptability in resources, process, training, and information sharing are key attributes of their operations.

Sector operations are personnel-driven, but highly dependent on communications, information technology, and transportation systems.
ESS personnel may maintain backup or redundant facilities, systems, and assets to maintain critical services during emergency incidents, and the sector is a restoration priority for other critical infrastructure services.

ESS personnel are operating in a limited resource environment.
Diminished government budgets may affect the capacity of the ESS to adequately address current risks as well as anticipate or prepare for changes to its risk profile.

EMERGENCY SERVICES SECTOR SNAPSHOT

COMPONENTS

Human

More than 2,500,000 career and volunteer ESS personnel in five disciplines

Law Enforcement

Emergency Management

Fire and Rescue Services

Emergency Medical Services

Public Works

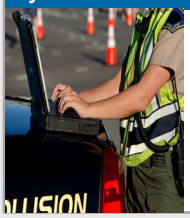
Physical

Facilities
for daily operations, support, training, or storage

Equipment
specialized for discipline and capability (e.g., personal protective, communications, surveillance)

Vehicles
specialized for discipline and capability (e.g., ambulances, HazMat, aircraft, and watercraft)

Cyber



Virtual Operations
Emergency operations communications, database management, biometric activities, and security systems are frequently operated in cyberspace.

Internet
The Internet is widely used by the sector to provide information and distribute alerts, warnings, and threats relevant to the sector.

Information Networks
Computer-aided dispatch and watch and warning systems, information-sharing portals, and social networking are leveraged to keep the ESS informed and connected.

PERSONNEL

- A majority of ESS personnel are SLTT employees and volunteers.
- Private sector ESS personnel include industrial fire departments, private security officers, and private EMS providers.
- The five ESS disciplines include approximately 1,200,000 Law Enforcement, 1,100,000 Fire and Rescue Services (the large majority of which are volunteer), 240,000 EMS (the large majority of which are volunteer), 9,000 Emergency Management, and 37,000 Public Works personnel.†

† ESS discipline totals are approximations from a combination of U.S. Department of Labor Bureau of Labor and Statistics data and discipline association Websites.

REGULATION AND PROFESSIONAL STANDARDS

- The sector as a whole, is not regulated; however, regulations govern many emergency response functions at the SLTT level (e.g., hazardous materials [HazMat], fire and rescue, public utility emergencies).
- HazMat-related Federal regulatory agencies include U.S. Environmental Protection Agency (EPA), Pipeline and Hazardous Materials Safety Administration, and Occupational Safety and Health Administration (OSHA).
- The National Fire Prevention Association provides numerous professional codes and standards for fire prevention and public safety that ESS disciplines use and reference.

CRITICAL SECTOR INTERDEPENDENCIES

Energy—Fuel and electric power are essential for ESS operations and the ability of critical infrastructure to respond to emergencies.

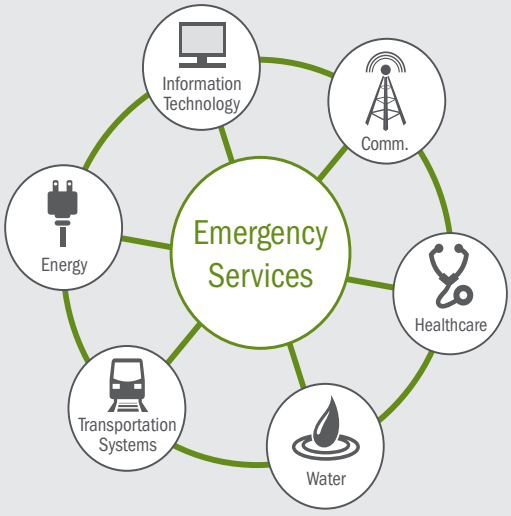
Communications—Radio spectrum networks and infrastructure enable ESS to carry out its mission.

Transportation Systems—Secure and effective movement of goods and personnel over multiple modes is required for emergency response and recovery.

Water—Water is critical for sustaining communities and infrastructure before, during, and after emergencies.

Healthcare and Public Health—First responders and EMS coordinate with the Healthcare Sector to respond to emergencies.

Information Technology—A variety of cyber-related assets, systems, and disciplines are increasingly essential to help ESS carry out its mission.



Sector Components, Disciplines, and Capabilities

Components

The ESS consists of systems and networks composed of physical, cyber, and human components.

Physical Component

The physical component includes the operations and storage facilities, specialized equipment, and vehicle fleets that enable personnel in each ESS discipline to perform critical services during steady-state and crisis operations. Specialized equipment and vehicles often require extensive personnel training and have distinct maintenance and storage requirements to ensure safe and effective operation when needed. Emergency communications equipment, such as land mobile radio systems, are a substantial physical component in any agency.

Cyber Component

ESS operations are increasingly dependent on complex information technology and cyber systems, particularly as security technologies advance. Emergency operations communications, database management, biometric activities, telecommunications, and electronic security systems are conducted virtually and are vulnerable to cyber disruptions. The sector widely uses the Internet to provide information, alerts, warnings, and threats to ESS and critical infrastructure partners. Degradation of the systems that support these activities would significantly raise the overall risk to a facility and individual emergency responders and could impede effective operations.

Human Component

The sector's most important component is the human assets—more than 2.5 million career and volunteer practitioners who serve in every community in the United States. These individuals contribute to the safety and security of the Nation by saving lives, preparing for and managing response operations, protecting residents and property, and ensuring public order in times of disaster.

Disciplines

Five distinct disciplines compose the ESS, encompassing a wide range of emergency response functions and roles.

Law Enforcement

Federal, SLTT, and private sector assets, networks, and systems (including physical, cyber, and human components) that contribute to public safety and quality of life by enforcing laws, conducting criminal investigations, collecting evidence, apprehending suspects, securing the judicial system, and ensuring custody and rehabilitation of offenders. Law enforcement consists of police departments, sheriff's offices, courts systems, correctional institutions, and private security agencies.

Fire and Rescue Services

Federal, SLTT, and private sector assets, networks, and systems (including physical, cyber, and human components) that contribute to public safety and quality of life through fire suppression, fire prevention, hazardous materials control, life and property safety operations (including technical rescue), building code enforcement, and fire safety education. Fire and rescue services consist of both paid and volunteer personnel.

Emergency Medical Services

Federal, SLTT, and private sector assets, networks, and systems (including physical, cyber, and human components) that contribute to public safety and quality of life through providing medical care at the scene of an incident, during an infectious disease outbreak, and during patient transport and delivery to a hospital or other treatment facility. Activities at incidents include handling the triage, treatment, and transport of injured and ill patients; taking appropriate steps to protect staff, patients, facilities, and the environment; and helping to monitor response teams while providing needed comprehensive medical care to patients. EMS consists of both paid and volunteer personnel.

Emergency Management

Federal, SLTT, and private sector assets, networks, and systems (including physical, cyber, and human components) that contribute to public safety and quality of life by providing incident management and coordination (including pre- and post-event activities) between ESS disciplines, as well as with non-emergency services entities. Emergency Operations Centers (EOCs) provide emergency management personnel with the capability for multiagency coordination for incident management by activating and operating for pre-planned or no-notice events. EOCs support the coordination of response and recovery activities among neighboring jurisdictions at various levels, as well as with Federal, SLTT, and private sector EOCs.

Public Works

Federal, SLTT, and private sector assets, networks, and systems (including physical, cyber, and human components) that contribute to public safety and quality of life through services such as assessing and repairing damage to buildings, roads, and bridges; clearing, removing, and disposing of debris from public spaces; restoring utility services; and managing emergency traffic. With responsibility for hardening security enhancements to critical facilities and monitoring the safety of public water supplies, public works is an integral component of a jurisdiction's emergency planning efforts. In addition, public works departments supply heavy machinery, raw materials, and emergency operators and may also manage contracts for additional labor, equipment, or services that may be needed before, during, and after an incident.

Specialized Capabilities

In addition to foundational capabilities of the disciplines, Federal, SLTT, and private sector assets, networks, and systems also provide specialized emergency services through individual personnel and teams. These specialized capabilities may be found in one or more various disciplines, depending on the jurisdiction:

Tactical Teams

Teams of personnel with specialized training, communications systems, vehicles, and equipment for specific duties, such as hostage rescue and counterterrorism operations, high-risk arrests, and entering armored or barricaded buildings. While traditionally a law enforcement capability, such as special weapons and tactics (SWAT), cross-training with fire and rescue personnel/functions and emergency medical services personnel/functions has recently increased.

Hazardous Devices Team/Public Safety Bomb Disposal

Teams of personnel with specialized training, communications systems, vehicles, and equipment for the rendering safe of actual and alleged explosive devices. Personnel are usually part of law enforcement or fire and rescue organizations.

Public Safety Dive Teams/Maritime Units

Teams of personnel with specialized training, communications systems, vehicles, and equipment for (under)water rescue, recovery, and investigation. Personnel are usually part of law enforcement, fire and rescue, or emergency medical services organizations.

Canine Units

Personnel with specialized training and equipment, specifically canines, for drug detection, explosive detection, cadaver detection, arson and accelerant detection, search and rescue, evidence search, suspect apprehension, and handler protection.

Aviation Units

Personnel with specialized training, communications systems, and equipment who utilize fixed- and rotary-wing aircraft for law enforcement, fire and rescue, emergency medical services, and emergency management functions.

Hazardous Materials

Teams of personnel that assess, mitigate, and manage the consequences of a hazardous materials (chemical, biological, radiological, or nuclear (CBRN)) incident.

Search and Rescue (SAR)

Teams of personnel with specialized training, communications systems, vehicles, and equipment to search for, treat, and rescue distressed individuals and groups, and recover decedents. Examples of SAR operations include structural collapse, confined space, vehicle, water, wilderness, trench and excavation, machinery, cave, mine and tunnel, helicopter, tower, and animal rescue.

Public Safety Answering Points

Personnel with specialized training, communications systems, and equipment used to receive requests for law enforcement, fire and rescue services, emergency medical services, emergency management, and public works assistance. Personnel receive requests from the public, other critical infrastructure sectors, or other organizations and then organize and relay these requests to the appropriate discipline.

Fusion Centers

Focal points within the State and local environment for the receipt, analysis, gathering, and sharing of threat-related information between the Federal Government and SLTT and private sector partners.

Private Security Guard Forces

Personnel who provide operational facility and site security to private sector and government facilities and operations.

National Guard Civil Support

Teams of full-time, State-level National Guard personnel with missions to support civil authorities in domestic incidents. National Guard teams provide engineering, transportation, medical, and aviation support for a variety of emergencies, including natural disasters, CBRN incidents, and structural collapses.

2.2 Sector Risks

The sector's large, geographically distributed base of facilities, equipment, and highly skilled personnel provide first response to nearly every critical infrastructure sector and every disaster imaginable. Sector personnel serve as the Nation's first line of defense in preventing and mitigating the effects of physical and cyber threats, whether natural or manmade—making them susceptible to all hazards and any type of incident. The sector's diversity in organization, mission, and assets makes disabling the entire emergency services system difficult. However, damage or disruption to ESS components can dramatically impede the protection of the public, other critical infrastructure sectors, and disciplines internal to the sector.

Notable Trends and Emerging Issues

Since the last SSP was issued in 2010, key changes in policy, resources, threat types, and public expectations have affected the sector's risk profile. The following eight trends and issues are key to sector partners as they adapt security and resilience efforts to evolving risks:

- **Increasing public expectations for ESS expertise, rapid response capabilities, and real-time information sharing**—Past ES SSPs have focused on mitigating specific types of threats, but the ESS has shifted focus to all-hazard incident response planning as threats rapidly evolve. This coincides with the public's increasing expectations for ESS personnel to respond with expertise to incidents of all kinds and provide constant real-time information sharing. Devoting personnel to meet public information needs can diminish the surge capacity of incident management teams, while public panic in the absence of information creates an additional burden on the ESS. A combination of decreased funding, increased mandates, and increases in training requirements and equipment maintenance costs compounds this added resource constraint.
- **Reduced grant funding constraining State and local resources**—Reductions in grant funding to State and local departments and diminished budgets may affect the capacity of the ESS to adequately address and anticipate or prepare for changes to its threat profile. Specifically, reductions have forced the ESS community to choose between terrorist threat mitigation strategies and traditional police activities, such as drug and gang enforcement. Costs have increased for healthcare, personnel, and fuel and maintenance for equipment. Further, as the demands for response increases, the risk of major events may consume disproportionately large amounts of supplies and equipment, which could limit the goods and services available to separate or multiple incidents.
- **Extreme weather events**—Frequent and extreme weather events will increase the response demands, which may drain sector personnel, assets, and capabilities. Natural disasters also threaten key services that enable ESS response.
- **Greater dependence on cyber infrastructure**—The ESS has become increasingly dependent on cyber assets, systems, and disciplines to carry out its primary mission to protect and respond to emergency incidents. Cyber technology advancements, such as the development of Next-Generation 9-1-1, the transition towards cloud-based information systems, and the usage of geospatial tools, have enabled the ESS to expand and improve its operations. However, new risks associated with such advancements, including data encryption limitations, location accuracy gaps, global positioning system (GPS) disruptions, driver distractions, and user information privacy issues, challenge the sector's capability to quickly and safely respond to emergencies.
- **Changing population dynamics**—Increased population density in urban and suburban areas and specific population characteristics (e.g., increasingly mobile and interconnected, new access and functional needs, language barriers) may exacerbate existing risks. The average age of the general public is increasing, which increases the frequency at which medical response is needed, and introduces additional requirements and complications for emergency

response. Transportation incidents are more frequent, which increases both the demand for HazMat-related response and the length of time needed to respond. Global mobility increases the risk of spread of biological agents and communicable diseases and related loss of able-bodied ESS personnel responding to those incidents.

- **Attacks targeting or compromising ESS personnel—**First responders are already at greater risk due to the nature of their work; however, ESS personnel may also become the target of attacks when responding to mass casualty, active shooter, or IED incidents, where an attacker's aim is to increase the amount of damage or number of casualties. Incident response may also affect the physical and emotional health of ESS personnel and their families.
- **Aging infrastructure—**Aging infrastructure throughout the United States—including electrical grids, water/wastewater systems, and roads and bridges—increases the risk of failure, which creates incidents that require ESS response while also impeding services critical to ESS functions.
- **Loss of workforce expertise—**As the average age of personnel across the sector increases, the ESS is at risk for losing key experience and expertise in its workforce due to retirement. Efforts to fill resultant vacancies may draw upon a pool of practitioners with much less experience.

Significant Emergency Services Sector Risks

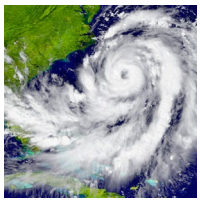
Given the critical mission of the ESS, risks to its operations and functions could prove disastrous to the safety and morale of the public, the protection of other critical infrastructure sectors, and the safety of its own disciplines. Below are four of the most significant sector threat vectors and their associated risks, which may be influenced or expanded by the issues discussed above. Many sector-specific threats are well-understood and the sector has taken considerable steps to mitigate known and evolving risks through partnership efforts—many of which are outlined in Chapter 3. The sector has used this risk profile to build its goals, priorities, and activities in Chapters 4 and 5.

Cyber Infrastructure Attacks or Disruptions

The ESS has become increasingly dependent on cyber-based infrastructure and operations, including emergency operations communications, data management, biometric activities, telecommunications (e.g., computer-aided dispatch), and electronic security systems. Because of this reliance, ESS cyber infrastructure may be a key target for cyberattacks (e.g., denial-of-service incidents and attacks on information systems and files) from anywhere in the world.

The increasingly interconnected nature, complexity, and need for constant availability of ESS information technology (IT) and cyber systems increases the cybersecurity risks to ESS communication systems and operations.

Natural Disasters and Extreme Weather (Earthquakes, Hurricanes, Fires, and Floods)



More extreme weather increases the geographic magnitude and severity of disasters, requiring a surge of ESS resources, often for extended periods, while also straining resources in partnering regions that might otherwise supply mutual aid. Disasters provide an increased hazard to responders, while often disrupting critical services needed for effective response.

Violent Extremist and Terrorist Attacks

Violent extremists—individuals who support or commit ideologically-motivated violence to further political goals—are increasingly targeting emergency services personnel, especially law enforcement, and soft targets.

The dynamic threat of terrorism persists and is becoming more diversified through a wide range of attack methods (e.g., IEDs, vehicle-borne IEDs, weaponized agents). Secondary explosive devices, which aim to harm the first responders to an initial incident, pose a specific threat to the ESS.

The Internet and social media increasingly enable lone actors and terrorists to identify and interact with others and obtain the ideological and material support needed for acts of violence.

Chemical, Biological, Radiological, and Nuclear Incidents

Emergency services personnel responding to and treating victims of CBRN incidents may also be at risk due to residual agents within the environment or on the victims and their clothing.

Biological agents or infectious disease can quickly spread through numerous jurisdictions and greatly strain emergency service resources and impact the health and safety of large numbers of the public and responders. The medical community and ESS personnel must receive appropriate instruction and messaging on quarantine and isolation measures.

Emergency services personnel may be exposed to unknown hazards when responding to HazMat incidents as cargo information provided to first responders may not always be accurate. Without this specific information, incidents could expand to affect larger areas and groups of people.

Like chemical and biological incidents, radiological and nuclear incidents require a great deal of technical training and specialized equipment for emergency services personnel. Shortages of critical resources may limit the capabilities to rapidly respond to and contain such incidents.

Cross-Sector Interdependency Risks

A degradation of ESS response capability would negatively affect a wide range of organizations and communities—the other 15 critical infrastructure sectors, Federal departments and agencies, SLTT governments, the private sector across industries— and public safety, security, and morale. In parallel, other critical infrastructure sectors provide services that are integral to the safety of ESS personnel and continued functioning of ESS cyber and physical assets. The most significant ESS critical infrastructure sector interdependencies are with the lifeline functions, which are listed below, followed by other interdependencies.

Internal Dependencies

Each ESS discipline depends on the services of other ESS disciplines for continued functioning. For example, law enforcement officers protect fire department and EMS personnel at the scene of an emergency, and public works personnel may need to clear debris from emergency routes to facilitate site access for first responders.

Lifeline Functions: Energy, Transportation Systems, Communications, and Water

ESS organizations rely on energy supplies to maintain critical operations during natural and manmade disasters and to fuel its service vehicle fleet.

The ESS depends on a resilient transportation network in order to effectively respond to emergencies. Response vehicles must be able to transport people, goods, and services to and from incident areas. This includes the movement of ESS assets to other geographical locations throughout the Nation.

The ESS relies on operational and public communications, such as through an internal communications network, 9-1-1 services, or other public alerting and warning systems.

The critical mission of providing emergency services, such as in firefighting and public works, requires a clean and reliable water supply.

Other Key Interdependencies

In responding to emergencies, first responders and EMS coordinate with the Healthcare Sector; law enforcement may provide security for various public health emergencies, such as mandatory quarantine or isolation orders or mass distribution of medication.

The ESS has become increasingly dependent on a variety of cyber-related assets, systems, and disciplines to carry out its mission. The loss of computer-aided dispatch services, the corruption or loss of confidentiality of critical information, or jammed/blocked surveillance capabilities could significantly disrupt the sector's capability to adequately protect the public and safely and quickly respond to emergencies.

2.3 Critical Infrastructure Partners

Protecting ESS assets, systems, and networks requires strong collaboration and partnerships among all levels of government, regional organizations, sector owners and operators, and associations that represent disciplines within the sector. Similar to the other critical infrastructure sectors, the ESS operates under the NIPP partnership structure, which employs public and private sector councils. The sector also uses the Critical Infrastructure Partnership Advisory Council framework to facilitate collaboration between government and private sector partners to inform critical infrastructure security and resilience efforts. Partnership councils meet throughout the year to exchange ideas and lessons learned; facilitate sector-level planning and resource allocation; establish effective coordinating structures; and develop security and resilience tools, guidelines, products, and programs.

Emergency Services Sector Partnership Structure

Figure 1: Emergency Services Sector Partnership Structure

Due to the critical mission of the ESS, there are many partners in Federal and SLTT departments and agencies, the private sector, non-profit or volunteer-based organizations, and trade associations. The full engagement of ESS partners in developing and implementing protective programs depends on understanding the benefits through participation in the partnership structure. ESS activities within the partnership structure provide an opportunity to work collaboratively to:

- **Improve Access to Threat Information—**DHS and the ES Sector-Specific Agency (SSA) work to improve access to timely and appropriate threat information for ESS partners to improve public safety and to enable proper protection of ESS critical infrastructure.
- **Improve Information Sharing—**Participation in the partnership enables information sharing and connections with ongoing initiatives, both public and private, through a collaborative forum designed to raise awareness and increase security.
- **Impact National Policy—**Through participation in the GCC or SCC, organizations and individuals have the opportunity to leverage their expertise to make substantive changes to national policy that reflect the role of the ESS as a critical infrastructure partner in homeland security.
- **Enhance Research and Development Support—**DHS and the ES SSA incorporate input from sector partners to help inform the sector and assist in the prioritization of R&D projects that may touch directly or indirectly on the activities of ESS personnel.
- **Focus Critical Infrastructure Activities—**The ES SSA and its sector partners participate in the development of resilience measures and strategies that focus on the organizational, jurisdictional, or discipline level and are designed to better inform resource allocation.
- **Increase Sector Resilience—**Participation in the partnership enables the development of a comprehensive risk management strategy to increase ESS resilience and security through improved access to tools, education, and training.

All ESS partners are urged to participate in sector efforts, communicate critical infrastructure security and resilience activities to appropriate representatives, and express their concerns to sector leaders who can advise them of appropriate channels to follow for problem resolution. By these means, the overall resilience posture of the ESS and the Nation's infrastructure security will be improved.

Sector-Specific Agency

The Office of Infrastructure Protection (IP) executes the role of SSA on behalf of DHS. The Assistant Secretary for Infrastructure Protection chairs the GCC and has designated the Director of the Sector Outreach and Programs Division as the representative on behalf of IP. The Director designates an alternate to assist as necessary. The SSA's responsibilities include leading, integrating, and coordinating the overall national effort to enhance ESS critical infrastructure resilience.

- Identify, prioritize, and coordinate the security and resilience of sector critical infrastructure with a particular focus on critical infrastructure that could be exploited to cause catastrophic health effects or mass casualties comparable to those produced by a weapon of mass destruction.
- Collaborate with sector partners, including facilitating information sharing and building critical infrastructure partnerships.
- Work with DHS components to develop, evaluate, validate, or modify sector-specific risk assessment tools.
- Assist sector partners in their efforts to organize and conduct security and continuity of operations planning, and to elevate awareness and understanding of threats and vulnerabilities.
- Identify and promote effective sector-specific critical infrastructure security and resilience practices and methodologies.
- Monitor and report on performance measures for sector-level NIPP 2013 implementation activities to enable continuous improvement of ESS security and resilience efforts.

Sector Partners

The ESS is expansive, with geographically distributed personnel and assets, and is primarily organized at the SLTT levels of government, corresponding to the typical scale of emergency occurrences. Strong collaboration requires partnerships encompassing not just Federal agencies and sector owners and operators, but also SLTT partners, regional organizations, trade associations, and advisory bodies (such as the InterAgency Board (IAB)). These entities provide a critical link for ESS personnel operating in an all-hazards environment within and across geographical areas.

The ES GCC provides effective coordination of security strategies and activities, policy, and communications across the Federal Government and between the government and sector stakeholders to support the Nation's homeland security mission. The GCC consists of members whose departments and agencies are integral to the sector and responsible for coordinating critical infrastructure strategies and activities, policy, and communication within their organizations, across government, and between governments and sector members. The GCC acts as the counterpart and partner to the ES SCC in planning, implementing, and executing sector-wide infrastructure programs.

The ES SCC is a self-organized, self-led body of ESS members who collaborate with the ES SSA, ES GCC, and Emergency Management and Response–Information Sharing and Analysis Center (EMR-ISAC) to address the entire range of infrastructure issues and activities, including sector-wide planning, development of sector best practices, sector-wide promulgation of programs and plans, development of requirements for effective information sharing, R&D, and cross-sector coordination. The SCC provides sector stakeholders with a venue to contribute their technical expertise and provides DHS with a reliable and efficient way to communicate and consult with the sector on programs and security issues. The SCC is organized through professional associations and associate members representing various types of emergency service providers. This organization supports a unified, interdisciplinary approach, powerful information dissemination to and gathering from emergency service workers, and the facilitation of sector collaboration and cross-sector outreach.

Visit the ESS Charters and Membership Webpage for the most up-to-date list of council members and charters.

Government Coordinating Council

United States Department of Homeland Security

- Office of Infrastructure Protection (Sector Outreach Programs Division, Protective Security Coordination Division, Infrastructure Security Coordination Division)
- Office of Cyber and Infrastructure Analysis
- Office of Cybersecurity and Communications
- Federal Protective Service
- Science and Technology Directorate
- Federal Emergency Management Agency (National Integration Center, Emergency Management Response Information Sharing and Analysis Center)
- Office of Health Affairs
- Office of State and Local Law Enforcement

United States Department of Justice

- Federal Bureau of Investigation

United States Department of Transportation

- National Highway Traffic Safety Administration

InterAgency Board

State, Local, Tribal, and Territorial Government Coordinating Council

Sector Coordinating Council

American Ambulance Association

American Public Works Association

Central Station Alarm Association

City of Winchester, Virginia

County of Story, Iowa Sheriff's Office

North County Fire Protection District

Electronic Security Association

Emergency Management Association of Texas

Emergency Preparedness Resource Group

International Association of Chiefs of Police

International Association of Emergency Managers

International Association of Fire Chiefs

National Association of Security Companies

National Association of State EMS Officials

National Emergency Management Association

National Fire Protection Association

National Native American Law Enforcement Association

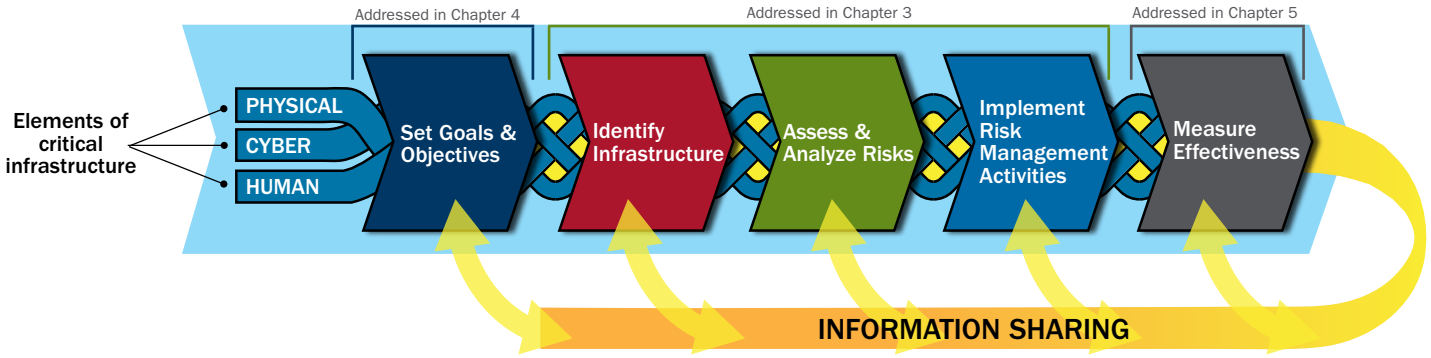
National Sheriffs' Association

Securitas Security Services

Security Industry Association

3 RISK MANAGEMENT AND NATIONAL PREPAREDNESS

Figure 2: NIPP 2013 Critical Infrastructure Risk Management Framework



The ESS goals and objectives are directly rooted in the NIPP 2013 risk management framework (Figure 2). Updated goals and objectives reflect the maturation of the partnership and the significant progress made toward 2010 SSP objectives. This chapter presents the sector's ongoing efforts and the planned approaches that support risk management and national preparedness, response, and recovery following an incident that affects ESS operations. For more information about sector resources, visit the Emergency Services Sector Webpage or email ESSTeam@hq.dhs.gov.

3.1 Accomplishments

The following major accomplishments are arranged by their alignment with components of the NIPP 2013 risk management framework:

Set Goals and Objectives

- Project Responder 3 (PR3) and Project Responder 4 (PR4), developed in 2012 and 2014, respectively, continue a series of studies begun in 2003 to focus on identifying capability needs, shortfalls, and priorities for catastrophic incident response. These studies were commissioned by DHS S&T and conducted through a collaboration between the Homeland Security Studies and Analysis Institute, DHS S&T First Responder Resource Group (FRRG), and the IAB. PR3 identified the highest priority capabilities of first responders to address the gaps established in 2004 and 2008. PR4 identified a set of enduring and emerging capability needs, framed them into technology objectives, and assessed the state of science and technology to meet those needs.
- The ESS formed a broad-based Credentialing and Disaster Reentry Working Group (CDRWG) in 2012 to respond to the Nation's need for a standardized, cross-jurisdictional approach to all-hazards/all-sectors crisis reentry for public and private emergency responders. This joint effort yielded the Emergency Responder Identity Trust Network (ER-ITN) and Crisis Reentry Joint Standard Operating Procedure (JSOP), which provide a consistent approach for ESS stakeholders to manage crisis reentry control through phased access and identity verification. The CDRWG is integrated with Federal policy and technology initiatives addressing first-responder credentialing and has influenced improvements to Federal policies on access credentialing.
- The ESS formed a Working Group on Medical Countermeasures in 2011 to respond to the lack of a national strategy protecting the health of emergency services personnel regarding major public health incidents such as pandemics.

Assess and Analyze Risks

- Recognizing that ESS personnel are increasingly adapting to the growing prevalence of and reliance upon digital technologies and other cyber infrastructure in the sector, the ESS has emphasized identifying the sector's cyber risks and mitigation measures since 2010. The sector released two documents—the 2012 *Emergency Services Sector-Cyber Risk Assessment* (ESS-CRA) and the 2014 *Emergency Services Sector Roadmap to Secure Voice and Data Systems* (Roadmap)—to establish baseline national-level cyber risk and identify risk mitigation strategies.[1]

- In 2010, the ESS developed a self-assessment tool for sector partners, intended to assist ESS organizations in assessing their current capabilities, enhancing information sharing, reducing risk, and increasing resilience through the establishment of a capabilities database and Sector Risk Profile. The ES SSA, in coordination with the ES SCC, is working to incorporate the functions of this tool into the IP Gateway.

Implement Risk Management Activities

- The ESS developed and conducted the Twisted Fate exercise in 2012 for first-responder chief officers and senior officials, focusing specifically on the ESS resilience and continuity of operations (COOP). The ESS also partnered with the Federal Emergency Management Agency (FEMA) Continuity of Operations Division to develop a COOP survey, which gathers information on how the ESS incorporates COOP planning into their emergency management operations.
- In 2011, the ESS achieved a 59 percent increase in the number of approved security clearances for SCC members and stakeholders sponsored by the sector, which will allow for increased information sharing and risk management across the ESS community.
- ESS professionals of the Emergency Services Coalition for Medical Preparedness acquired information on new medical treatments to ensure the safety and resilience of sector personnel during an ESS response to biological incidents.

3.2 Risk Management

Under the NIPP 2013 framework, risk is the potential for an adverse outcome from an event, determined by the event's likelihood—a function of the specific threats and vulnerabilities—and associated consequences if the event occurs. While individual owners and operators are responsible for managing risk to their individual assets, ESS partnership activities can improve understanding of threats, vulnerabilities, and consequences and provide owners and operators with tools, guidelines, information, best practices, and resources to facilitate more effective risk assessments and risk management decisions at the facility and sector level.

The ESS is a composite sector with five disciplines engaged in an all-hazards mission. The sector is composed of assets, systems, and networks that contain physical, cyber, and human components. To manage risks throughout the sector, sector partners collaboratively undertake the critical infrastructure risk management framework process. The ESS risk management process entails identifying critical infrastructure, assessing and analyzing risk, and implementing informed risk management activities. Information is shared throughout the process to not only facilitate the decision-making process, but to also document and build upon best practices and lessons learned to identify and address gaps in security and resilience efforts.

The critical infrastructure risk management framework is the foundational approach to risk management and enables sector partners to have a common understanding and approach to managing risk. Although a common approach to risk management is taken, the complexity of the sector's structure may at times necessitate a more tailored approach through an asset-by-asset or mission approach to risk management. Throughout the sector, many SLTT government and private sector partners adapt the sector's foundational risk management methodology toward specific needs or apply it on an asset, system, network, or functional basis depending on the risk mitigation strategy. An example of Federal resources for supporting risk management is the National Institute of Standards and Technology (NIST) Cybersecurity Framework, which can be utilized by sector stakeholders as a reference for understanding cyber risks. Asset identification, risk assessment, informed risk management activities inclusive of asset prioritization, and consistent information sharing position the ESS to properly manage risk throughout the sector.

Identify Infrastructure

ESS assets, systems, and networks comprise physical, cyber, and human components, each of which contains a variety of specific elements that contribute to the function and protection of the sector (see the sector snapshot). To ensure effective critical infrastructure activity and resource management, the ESS must be able to identify, gather, validate, and update pertinent information on the sector's assets, systems, and networks. The key is to identify the specific infrastructure components that, in their incapacitation or destruction, would result in a debilitating impact on the Nation's security, national economic security, national public health and safety, or public confidence. This perspective of infrastructure criticality is not confined to the national level, but is also present at the regional, State, and local levels.

 **PHYSICAL** Equipment and materials, facilities, conveyances, and records that support or provide protection for the ESS.	**Equipment and Materials**—Unique devices, parts, or pieces of equipment including key elements of communications systems.
	Facilities—Physical structures that house or directly support ESS personnel, equipment, conveyances, records, and cyber elements.
	Communications Facilities—Communications infrastructure used by ESS providers to enable effective steady-state and incident communications, information exchange, and interoperability.
	Conveyances—Vehicles used to carry out critical ESS functions; for common ESS conveyances, information is defined by asset class, rather than by individual asset.
	Records—Documents in non-electronic media, including sensitive or classified government information, personnel records, accountability records, equipment inventory, financial information, and personally identifiable information.
 **CYBER** Hardware and software components that are critical to supporting the ESS mission, including computers, servers, databases, and other IT systems and assets used in ESS activities and typically fulfill one of four roles.	**Access Control**—Limits physical access to defined areas of a facility to authorized personnel and visitors only.
	Control Systems—Monitor and control sensitive processes and physical functions.
	Warning and Alert—Sends alerts and notifications with critical information that triggers protection and response actions.
	Data Collection Systems—Collect data for record retention and information sharing.
 **HUMAN** Personnel with unique training, certification, knowledge, skills, authorities, or roles, and whose absence could cause undesirable consequences or hamper the sector's mission.	**Strategic Positions**—Individuals who must be identified, assessed, and prioritized for protection to ensure continuity of essential government operations. Often includes the leadership of the ESS.
	Operational Positions—Individuals who operate critical infrastructure systems that, if impaired, could result in either cessation or takeover of operations, or, if compromised, would make recovery more difficult.
	Specialized Response Units—Personnel teams trained to carry out specific emergency response functions.
	Mutual-Aid and Multi-Agency Coordination—Formal and informal agreements and processes designed to connect agencies in different jurisdictions and enable a coordinated response to emergencies.

Asset Identification and Collection Tools

Infrastructure criticality is viewed differently across jurisdictions and area of responsibility based on each sector partner's unique situation, operating models, and associated risk. The Federal Government works with sector partners to determine which assets, systems, and networks are nationally significant and provides support to cooperatively identify regional, State, and locally significant infrastructure. SLTT governments represent the majority of the ESS and, therefore, have the best understanding of those assets, systems, and networks which are crucial to their continued operations, the sector's provision of essential services, and the safety of the sector. The Federal Government, SLTT agencies, and private industry utilize personnel and a variety of processes and tools to identify critical assets, systems, and networks in the ESS and collect this information in databases. In addition, the GCC and SCC identify additional means for data collection. Various tools for identifying assets include:

- **SLTT Government Identification**—SLTT entities utilize existing liaisons, partnerships, and councils to leverage the knowledge of SLTT government and sector subject matter experts to identify critical infrastructure assets.

- **SLTT Critical Infrastructure Asset Systems**—Asset systems developed and managed by SLTT agencies identify, prioritize, and assess risks to the State's critical infrastructure. These systems enable ESS partners to respond to national data calls by compiling asset information and integrating geospatial information statewide. They can also enhance ESS incident command capabilities and preparedness.
- **Federal Capabilities**—SLTT entities and other sector partners leverage the expertise of Federal Government partners, including DHS Protective Security Advisors (PSAs) and SSAs, to work together to build and update inventories of assets significant at various government levels.
    - **ESS-CRA**—Describes the cyber risk profile of the sector, which stakeholders can use to identify cyber assets.
    - **IP Gateway**—ESS sector partners can use IP Gateway to input and retrieve critical infrastructure information. IP Gateway also enables comprehensive vulnerability and risk analysis through the Infrastructure Survey Tool and other assessments, analytical products, and reports.
    - **National Counter-IED Capabilities Asset Database (NCCAD)**—Accumulates and analyzes data from bomb squads across the country to determine overall bombing prevention capabilities.

Critical infrastructure information submitted to DHS is considered sensitive and proprietary and is protected from public disclosure to the maximum extent permitted by law.[2] For verification and notification of needed updates, the SSA relies on owners of the sources and databases from which the information is gathered because of the sector's breadth and variety of information sources. Recognizing the challenges in verifying and updating infrastructure information, the SSA will work with sector partners, including the SCC and GCC, to determine appropriate mechanisms and procedures to ensure accurate, complete, and updated infrastructure information.

Identify Dependencies

In addition to understanding criticality, the risk management process entails an understanding of the associated interdependencies within the ESS. In order to comprehend the consequences of a disruption or attack on an asset, the ESS seeks to identify not only dependencies, interdependencies, and cascading effects both at the sector and asset levels, but also redundancies or mitigation/resilience activities to protect against catastrophic failure by actively sharing information and building relationships and partnerships across disciplines and jurisdictions. Many assets within the ESS depend on the lifeline functions of communications, energy, transportation systems, and water to maintain the sector's functionality. But, in addition to these external dependencies, the ESS also includes internal dependencies as disciplines depend on one another to carry out emergency functions. Each ESS discipline relies on other disciplines to develop associated and interdependent resilience strategies to minimize disruptions and their cascading effects. Furthermore, SLTT entities within the ESS use exercises and training to identify key lifeline sector interdependencies and enhance preparedness for all-hazards incidents.

Assess and Analyze Risks

The risk assessment is the cornerstone of the risk management framework, and the ESS utilizes a variety of assessment methodologies to implement the framework. The foundational critical infrastructure risk management framework enables ESS disciplines to operate with a common understanding of risk while retaining the flexibility to tailor the framework toward specific functional needs or assets, systems, and networks. Beyond the general purpose of critical infrastructure security and resilience, the information from risk assessments is used to prioritize risk management activities and can influence resource and budget decisions. To identify, evaluate, and mitigate threats, vulnerabilities, and consequences, the ESS utilizes a variety of risk assessment tools.

Risk Assessment Tools

The risk management framework employed throughout the ESS operates from a point of common understanding and terminology, despite the varying conceptualizations of infrastructure criticality across disciplines and jurisdictions. Although national-level assessments, such as the Strategic National Risk Assessment, are crucial to the comprehensive understanding of national risk, the ESS primarily conducts risk assessments at the State and local level focusing on assets and capabilities. Assessments conducted by the ESS adhere to several risk assessment methodology guidelines:

- **Documented**—Information used in the assessment and how it is synthesized to generate a risk estimate is documented and transparent to the user and others using the results.
- **Reproducible**—Despite variance in each discipline's facilities, capabilities, and personnel, the results are comparable and repeatable. Subjective judgments are minimized to allow for future policy and value judgments by owners and operators.
- **Defensible**—Assessment components are logically integrated and ESS disciplines are used appropriately to the risk analysis with a parallel effort to accomplish assessment accuracy and transparency.

Assessments completed within the sector are used by the sector as an ideal starting point for assessing risk in terms of threats, vulnerabilities, and consequences. Risk assessments are conducted by sector partners to meet a variety of decision-making needs and include the following assessment tools:

- **SLTT Hazard Identification and Risk Assessment (HIRA)**—SLTT ESS partners conduct HIRAs to understand and examine specific potential or existing circumstances that can generate a disaster or emergency incident at the SLTT level. HIRAs focus on quantitative assessment of hazards and consequences.
- **Threat and Hazard Identification and Risk Assessment (THIRA)**—Expands on HIRAs by broadening what is considered throughout the risk assessment process. SLTT entities use the THIRA process to complete the following qualitative risk assessments steps: identify the threats and hazards of primary concern to the community, develop threat and hazard context, establish targets for each core capability within the National Preparedness Goal, and apply the results to estimate resources required.
- **Enhanced Critical Infrastructure Protection (ECIP)**—Facilitates outreach to establish or enhance the relationship between DHS and critical infrastructure owners and operators. Voluntary security surveys are offered as a result of the outreach and are conducted by DHS PSAs to assess the overall security and resilience of the Nation's most critical infrastructure sites.
- **Onsite Assessments**—SLTT entities deploy onsite risk assessment teams that focus on high priority assets within their area of responsibility (AOR). Many risk assessment teams concentrate on critical infrastructure vulnerability and provide recommendations to the owner/operator to address potential threats and security vulnerabilities. An example of an available Federal onsite assessment is the Cyber Resilience Review—a no-cost voluntary cyber risk assessment facilitated by DHS cybersecurity professionals.
- **Planning Efforts**—Joint committees, such as local emergency planning committees (LEPCs), primarily comprise local emergency services representatives familiar with a variety of jurisdiction-specific risk factors. LEPC meetings are open to all emergency management stakeholders and enable the illumination of risk factors that may be inadvertently excluded from assessments. Some sector partners also rely on capital budgeting plans to determine if the organization's risk management investments are worth pursuing.
- **Cybersecurity Assessment and Risk Management Approach (CARMA)**—Provides a strategic methodology to identify, assesses, and manage cyber critical infrastructure risks in the sector.

Assess Vulnerabilities

A vulnerability is defined as the physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard. In addition to overall risk assessments, ECIP outreach and surveys, including the Infrastructure Survey Tool, are available to ESS partners to assess vulnerabilities. This security survey collects, processes, and analyzes facility assessment data in near-real time. The collected data is then weighted and scored to develop metrics, conduct sector-by-sector and cross-sector vulnerability comparisons, identify security gaps and trends across critical infrastructure sectors and subsectors, establish sector baseline security survey scores, and track progress toward improving critical infrastructure security through DHS IP's programs, outreach efforts, and training. Some sector partners also utilize a repurposed Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability (CARVER) method to assess the vulnerability of their assets, systems, and networks.

Assess Threats

A threat is defined as the natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property. When assessing risk, the threat of an intentional hazard is estimated as the likelihood of an attack that accounts for both the intent and capability of the adversary. In assessing threats, the ESS considers the full spectrum of intentional and unintentional threat sources, including natural threats (e.g., hurricane, fire, and floods), manmade threats (e.g., chemical, radiological, and biological attacks), workforce threats (e.g., pandemic flu, insider threat, and human error), and cyber-related threats (e.g., technological hazard and degradation). Within the ESS, the assessment of natural threats is more defined as natural hazards are more predictable based on the availability of historical data. Manmade threat sources are more complex. In the assessment of terrorist threats, ESS considers both capability and intent as discrete subcomponents of threat. The NIPP 2013 defines threat capability as the availability or the ease of use of tools or methods that could potentially be used to damage, disrupt, or destroy critical functions.

The ESS analyzes all types of applicable, potential threats and determines those of national and regional significance for inclusion within the threat portion of the sector's risk assessment. Threat assessments are most effective when applied to a specific threat source in a specific geographic region, State, or locality. The ESS leverages several threat assessments:

- **SLTT Fusion Center Threat Assessments**—Sector partners leverage fusion center and law enforcement-generated threat assessments and analyses. Fusion centers combine real-time threats with risk information, such as historical risk, in a timely manner; thus, enabling the ESS to effectively manage their security posture.
- **Federal Threat Assessments**—The ESS also utilizes threat sources and analysis from the Federal Government, including the National Infrastructure Simulation and Analysis Center, the Office of Cyber and Infrastructure Analysis, the DHS Office of Intelligence and Analysis, and the Federal Bureau of Investigation (FBI). Information-sharing portals, such as the DHS Homeland Security Information Network (HSIN) and the FBI's Guardian Program, are leveraged by sector partners as mechanisms to share threat-related information.

Assess Consequences

A consequence is defined as the effect of an event, incident, or occurrence that reflects the level, duration, and nature of the loss resulting from the incident. Consequences commonly include four components: public health and safety, economic, psychological, and governance or mission impact. The assessment of consequences is crucial to the risk management decision-making process. The multidirectional interconnections within the ESS and across other critical infrastructure sectors can produce complicated consequences at the local level within the sector. Although consequence factors have not been definitely determined by the sector, the following elements are generally considered when developing consequence:

- **Public Health and Safety**—Refers to the effect on human life and physical well-being (e.g., fatalities, injury, or illness). This element is measured by the number of lives affected or population at risk, as well as a unit of time during which the event negatively impacts the element or region (e.g., delays in response capacity or delivery of goods and services). It may be reduced by the amount of redundancy and resilience supplied by other responding elements.
- **Economic**—Refers to the direct and indirect economic losses, which include the cost to rebuild the asset, cost to respond to and recover from the incident, downstream costs resulting from the disruption of a product or service, and long-term costs due to environmental damage. This element is measured by the direct cost to replace a facility, responding capability assets, or the cost incurred in training, re-supply, or recovery of a capability element. It is expressed in dollars and can assist in deciding which mitigation efforts to implement and the prioritizing of critical elements.
- **Psychological**—Refers to the effect on morale and confidence in national economic and political institutions, including changes in perceptions emerging after a significant incident that affects individuals' sense of safety and wellbeing and may result in aberrant behavior. This element is difficult to measure with any degree of certainty.
- **Governance/Mission Impact**—Refers to the effect on the government or industry's ability to maintain order, deliver minimum essential public services, ensure public health and safety, and carry out national security-related missions. This element is measured in an increased response time or in the decreased abilities of surrounding capability elements to respond. Mission impact will have some degree of cascading effect to other sectors.

Assess Dependencies

The ESS possesses internal (e.g., among disciplines) and external (e.g., among other critical infrastructure sectors) dependencies and interdependencies, which expose the sector to potential cascading effects. To mitigate adverse cascading effects, the ESS relies on proven planning methods, exercises, and external knowledge input.

- **Planning Methods**—As part of the COOP process, sector partners are able to consider and assess the impact of dependencies that may affect their ability to continue their essential functions. FEMA's consequence management planning efforts provide a framework for not only developing supplemental emergency operations plans, but also planning for incident consequences and the impact on ESS infrastructure.
- **Exercises**—Scenario-based exercises allow for a dynamic discussion, which uncovers dependencies and provides a better understanding of potential cascading effects.
- **External Knowledge Input**—To varying degrees, sector partners rely on the Federal Government to provide input as to which dependencies are the most critical, as well as to make cascading effects evident across the diverse sector.

Implement Risk Management Activities

Each factor of the risk equation (vulnerability, threat, and consequence) and the relative importance of existing risk management gaps are considered when determining the prioritization of protective initiatives. To ensure the sector applies resources in areas that will best enhance the mitigation of risk, ESS infrastructure and associated security and resilience programs must be prioritized based on risk. Affordability, return on investment, and sustainability are key considerations in determining which resource shortfalls will be addressed immediately or over time.

Systematic methods for assessing the sector's assets, systems, and networks offer direction for decision-making and increase the defensibility of resource allocation decisions. Each ESS discipline may prioritize risk management activities based on activity costs, potential for risk reduction, and varying levels of infrastructure criticality—shaped by different views across jurisdictions and AOR. Although ESS disciplines hold a shared understanding of risk management and a common operating picture, differences in discipline mission, approach to risk, and tools used can manifest variances in the prioritization of critical infrastructure security and resilience activity within the sector. Future assessment tools can enhance the risk management activity prioritization and implementation process by ensuring comparable system information across the sector's critical infrastructure.

Adaptable and Coordinated Risk Management Prioritization

The ESS is made up of diverse disciplines and supporting elements with individual missions that address a wide variety of threats. The loss of ESS assets, systems, and networks ultimately results in a negative impact to the public from either delayed ESS response or no response to an attack, natural disaster, or other emergency. Without prioritized measures in place to secure its assets, systems, and networks, the sector cannot fulfill its critical mission. The ESS operates in a dynamic environment wherein threats, vulnerabilities, and consequences can vary over time and necessitate a continuous cycle of risk and capability assessment updates to ensure that operational decisions are grounded in superior situational awareness. As risk evolves, prioritization and protection choices should change accordingly. The ESS leverages planning committees, working groups, partnerships, and SLTT governments as instruments to discuss the prioritization of the sector's critical infrastructure and its activities.

Informed Risk Management Activities

Similar to the risk prioritization process, the ESS utilizes the information from risk assessments to inform the selection and implementation of risk management activities and national preparedness core capability priorities. Effective risk management activities are not only informed by risk assessments, but they are also comprehensive, coordinated, and cost-effective. To properly manage sector-wide risk management efforts traversing five disciplines, the unique concern of each ESS discipline introduced throughout the risk management approach is considered and used to inform and support the decision-making process. Federal risk management tools, such as ECIP visits and security surveys, benefit individual sector partners, as well as collective ESS risk management activities. These tools encourage voluntary and interactive stakeholder involvement and allow for a coordinated effort among sector partners, by collecting and sharing common risk gaps, obstacles, and protective measures.

Sector partners rely on different approaches to select risk management activities according to their specific authorities, missions, needs, risk landscapes, understanding of criticality, and approach to security and resilience. A variety of methods inform the evaluation and selection of risk management activities: risk assessments, strategic planning, stakeholder input, standards and best practices, lessons learned from actual events and exercises, measures effectively applied in similar settings, and risk modeling. ESS risk management activities can address multiple aspects of risks, while other activities may involve a more targeted tactic to address specifically identified threats, vulnerabilities, or potential consequences. There are three primary approaches to ESS risk management activities:

- **Identify, Deter, Detect, Disrupt, and Prepare for Threats and Hazards**—For example, establishing and implementing joint ESS plans and processes to evaluate needed increases in security and resilience measures based on hazard warnings and threat reports.
- **Reduce Vulnerabilities**—For example, developing and conducting training and exercise programs to enhance awareness and understanding of common vulnerabilities.
- **Mitigate Consequences**—For example, sharing information to support situational awareness and damage assessments of cyber and physical critical infrastructure during and after an incident, including the nature and extent of the threat, cascading effects, and the status of the response.

Training and Exercises

The delivery and continued development of effective training and exercises is critical to the execution and sustainment of the sector's risk management activities. To ensure the coordinated development and delivery of training and exercises, the ESS uses the following strategies:

- Capture, report, and prioritize needs of sector partners.
- Examine and leverage current Federal programs for use in the ESS.
- Leverage a network of sector partners to best serve sector partners and reach a wider audience.
- Partner with academia to inform critical infrastructure-related curricula, as well as to educate and train ESS professionals.

Throughout the approach to risk management, sector partners implement a variety of training and exercise programs to strengthen the sector's security and resilience capabilities.

- **Training**—The majority of training for ESS personnel is professional-based, including certifications according to discipline or specialized capability. Additional training programs offered by the Federal Government include the Office for Bombing Prevention's Counter-IED & Risk Mitigation Training; United States Fire Administration (USFA) support, training, and assistance to fire service operations and response; and FEMA Emergency Management Institute training courses on disaster prevention, protection, mitigation, response, and recovery.
- **Tabletop Exercises**—The Emergency Services Sector-Specific Tabletop Exercise Program enables sector partners to develop interactive and discussion-based exercises at the sector or facility level. The program is a flexible tool that includes pre-built exercise templates that can be tailored to address discipline-specific needs in order to assess, develop, and update their plans, programs, policies, or procedures.

Information Sharing

Information sharing is critical to a common operating picture, especially during incidents of national significance or affecting multiple jurisdictions simultaneously. Broad and deep information-sharing initiatives are crucial to ensuring information flows across Federal and SLTT levels and to the private sector, as appropriate. Information-sharing initiatives are augmented by ESS association Web sites and conference presentations. In addition, the GCC and SCC conduct regularly scheduled meetings and conference calls where security and resilience programs are discussed relative to strategies affecting a specific discipline or the ESS as a whole.

Federal Information Sharing

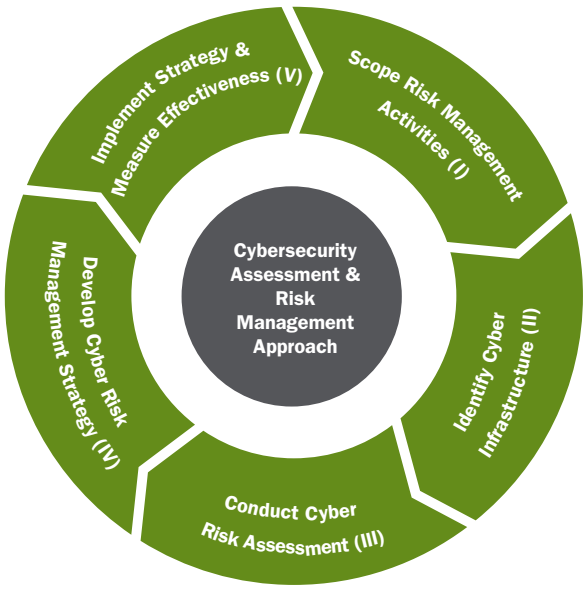
The SSA utilizes a variety of mechanisms to disseminate information to ESS stakeholders, such as Critical Infrastructure Partnership conference calls, coordinating information calls with Federal partners responding to incidents, and posting information to the Homeland Security Information Network–Emergency Services (HSIN-ES) portal and TRIP*wire* (Technical Resource for Incident Prevention). By ensuring information is readily available and easily accessible, HSIN-ES provides a valuable method to share up-to-date For Official Use Only and incident information with SCC members and sector stakeholders. Classified information sharing is further enhanced by the increase in the number of approved security clearances for SCC members and stakeholders sponsored by the sector through the Private Sector Security Clearance Program.

The SSA also coordinates with the EMR-ISAC, managed by the USFA Critical Infrastructure Program, to align and coordinate initiatives across the sector and to improve information sharing and connectivity. Critical infrastructure and emerging threat information is collected by the EMR-ISAC, which shares and disseminates it to ESS departments and agencies nationwide. Shared information frequently originates from other sectors. For example, information on resources regarding the Chemical Facilities Anti-Terrorism Standards program was distributed through the ISAC. EMR-ISAC also routinely publishes weekly articles on protection of critical infrastructure and emergency responders and bulletins containing critical homeland security information affecting ESS departments and agencies.

SLTT Information Sharing

Information sharing at the SLTT level incorporates Federal information-sharing mechanisms with daily coordination conducted primarily through SLTT fusion centers, many of which co-locate with SLTT critical infrastructure programs and law enforcement agencies. This proximity results in strong partnerships and close collaboration at the SLTT level. In addition, fusion centers and Federal Government entities with information-sharing missions have established liaison programs that further supplement information-sharing efforts. During emergency incidents, Emergency Operation Centers (EOCs) activate to address the emergency response and short-term recovery information-sharing needs of specific incidents and lead information-sharing efforts. These centers operate in a physical location, but also connect virtually through Internet-enabled platforms, such as WebEOC. The most effective way for Federal and SLTT information to reach the private sector is through time-tested proven mechanisms, such as fusion center bulletins, liaison programs, HSIN, FBI InfraGard chapters, regional forums, and trade associations.

Figure 3: The Five Stages of CARMA



3.3 Managing Cyber Risks

In addition to physical threats, the ESS also faces cyber threats from criminals, hackers, terrorists, and nation-states with varying degrees of capability and intention to attack ESS disciplines. Although the sector's existing security capabilities mitigate some cyber threats, the ESS is increasingly dependent on technology which can be increasingly vulnerable to exploitation and have negative implications sector-wide. To identify and manage these risks at a sector level, the ESS uses the DHS Office of Cybersecurity and Communications (CS&C) Cybersecurity Assessment and Risk Management Approach (CARMA), which is a five-step comprehensive, functions-based cyber risk management strategy that identifies, assesses, and manages shared risks for the sector's cyber critical infrastructure. As part of the CARMA process, the ESS has completed the ESS-CRA and Roadmap and plans to continue to work with CS&C to address a long-term work plan, implement the strategy and measure its effectiveness, and conduct cyber risk assessments.

The ESS also collaborates with CS&C to provide cybersecurity Webinars to its partners, conduct cybersecurity assessments, enhance cybersecurity implementation through Cyber Resilience Reviews, and promote and develop cyber risk management strategies and partnerships through the DHS critical infrastructure cybersecurity program. ESS's collaborative approach to cyber information sharing and cybersecurity is supported by HSIN-ES and working groups responsible for information sharing and cybersecurity. Cyber-related alerts and resilience strategies are disseminated throughout the sector through the Multistate Information Sharing and Analysis Center, the EMR-ISAC, and the U.S. Computer Emergency Readiness Team (US-CERT).

Emergency Services Sector Cyber Risk Assessment

Effective sector-wide cyber risk assessments evaluate the cybersecurity threats, vulnerabilities, and consequences associated with the critical functions and services the sector provides. The Emergency Services Sector Cyber Risk Assessment (ESS-CRA) provides a cyber-risk profile that ESS partners can use to enhance their security and resilience. This risk profile can also be used by ESS partners to prioritize how they spend resources and where to focus training, education, equipment, investments, grant requests, and further studies. The assessment identified threats to voice, data, and video communications systems and networks as the most likely threat to ESS cyber resources and included seven distinct cyber event scenarios that could significantly affect the ESS's ability to effectively perform its responsibilities. The scenarios enabled participants to discuss practical discipline implications while allowing for consideration of compounding and overlapping effects that often spread across multiple disciplines' cyber infrastructure.

Emergency Services Sector Roadmap to Secure Voice and Data Systems

The acquisition of new technologies allow for greater communications, collaboration, and cooperation among sector disciplines, but have illuminated new risks that require a more systemic response to cyber risk. The Roadmap proposes several risk mitigation measures to address the cyber risks identified in the ESS-CRA and provides justification for the response, sector context, and implementation barriers and suggestions. The Roadmap outlines the full range of risk mitigation measures that ESS disciplines can apply and provides an improved means of reducing cyber risk throughout the ESS. The risk mitigation measures are presented within five segments: preserving and protecting citizen access to emergency services, protecting facility and cyber infrastructure capabilities, planning and preparing for cyber incidents, using and assuring public alerting and warning systems, and defending surveillance systems and networks.

National Institute of Standards and Technology Cybersecurity Framework

In response to EO 13636: Improving Critical Infrastructure Cybersecurity, NIST developed a Framework for Improving Critical Infrastructure Cybersecurity, in addition to a companion roadmap. The framework consists of standards, guidelines, and practices (including public-private coordination through the Critical Infrastructure Cyber Community Voluntary Program) that can assist critical infrastructure owners and operators in managing cyber-related risk. Pursuant to the Roadmap to Secure Voice and Data Systems, ESS discipline leadership will determine the standards recommended by such bodies as NIST in regards to organizational responsibilities for implementing cybersecurity policies and procedures.

3.4 Mitigating Disruptions from the Loss of Lifeline Functions

All critical infrastructure sectors rely on the security and availability of certain lifeline functions that are essential to sector operations. These lifeline functions include aspects of communications, energy, transportation, and water. Disruptions in these lifeline functions not only may hinder the ability of the ESS to perform its mission to serve, protect, and aid, but also may cause impacts that cascade to other sectors, services, or functions critical to communities, regions, or the Nation. In planning and preparing for—and responding to—emergencies, the ESS strives to mitigate the impacts of such disruptions through a variety of means, including:

- Maintaining redundant communications systems and equipment for the continuous flow of emergency information.
- Coordinating fuel and power availability with Energy Sector partners for emergency services.
- Leveraging ESS assessment tools to identify available resources and potential lifeline function points of failure (more information on sector assessment tools can be found in Section 3.2 Risk Management).
- Developing and implementing mutual aid mechanisms between ESS disciplines and sectors that provide lifeline functions so that disruptions can be more readily absorbed and addressed.
- Engaging in robust training and exercises to expand the understanding of lifeline function disruption consequences and establish effective mitigation practices.

3.5 Research and Development Priorities

R&D plays a critical role in enabling homeland security partners to develop knowledge and technologies that more effectively reduce risk to the ESS. New and innovative technologies are required in order to maintain a strategic position in

preventing and mitigating the potential effects of current and future dangers. A comprehensive R&D approach supported at the Federal level and encompassing both operational and critical infrastructure R&D needs best enables the ESS to address current and future dangers. Primary efforts in this prioritization process include:

- The National Critical Infrastructure Security and Resilience Research and Development Plan (National CISR R&D Plan) identified five cross-sector R&D priority areas that are intended to inform R&D investments, promote innovation, and guide research across the critical infrastructure community. The ESS plans to work closely with its Federal partners to support National CISR R&D Plan implementation. The National CISR R&D Priority Areas include:
  - Develop the foundational understanding of critical infrastructure systems and systems dynamics.
  - Develop integrated and scalable risk assessment and risk management approaches.
  - Develop integrated and proactive capabilities, technologies, and methods to support secure and resilient infrastructure.
  - Harness the power of data sciences to create unified, integrated situational awareness and to understand consequences of action.
  - Build a crosscutting culture of CISR R&D collaboration.
- The DHS S&T First Responders Group (FRG) uses a solution development process to help determine the priority needs of first responders. Specifically, the FRG identifies, validates, and facilitates the fulfillment of first responder capability gaps through the use of existing and emerging technologies, knowledge products, and the acceleration of standards. The FRG, which includes DHS operational components and SLTT representatives from the first responder community, aids DHS S&T by identifying capability gaps and providing operational requirements for first responder R&D efforts.
- The IAB supports R&D efforts by providing Federal partners a prioritized, cross-cutting view of critical issues in technology and R&D related to the ESS.
- Coordinating R&D efforts is challenging for a sector comprising five disciplines with numerous stakeholders, assets, and priorities. DHS IP recognizes this challenge and provides assistance to SCCs, GCCs, and SSAs in identifying and meeting their R&D requirements. The SSA works with these entities to ensure the priorities meet the strategic needs of the sector and to prevent duplication, overlap, and omission.

The IAB and FRG collaborated in 2014 to identify the following key R&D capability priorities, which are also included in Project Responder 4.

Situational Awareness

- The ability to know the location of responders and their proximity to risks and hazards in real time.
- The ability to detect, monitor, and analyze passive and active threats and hazards at incident scenes in real time.
- The ability to rapidly identify hazardous agents and contaminants.
- The ability to incorporate information from multiple and nontraditional sources (e.g., crowdsourcing and social media) into incident command operations.

Communications

- The ability to communicate with responders in any environmental condition (including through barriers, inside buildings, and underground).
- Communications systems that are hands free, ergonomically optimized, and can be integrated into personal protective equipment.
- Command, control, and coordination.
- The ability to remotely monitor the tactical actions and progress of all responders involved in the incident in real time.

- The ability to identify trends, patterns, and important content from large volumes of information from multiple sources (including nontraditional sources) to support incident decision-making.
- The ability to identify, assess, and validate emergency-response-related software applications.

Responder Health, Safety and Performance

- Protective clothing and equipment for all responders that protects against multiple hazards.
- Logistics and resource management.
- The ability to identify what resources are available to support a response (including resources not traditionally involved in response), what their capabilities are, and where they are in real time.
- The ability to monitor in real time the status of resources and their functionality in current conditions.

Casualty Management

- The ability to remotely scan an incident scene for signs of life and decomposition to identify and locate casualties and fatalities.

Training and Exercise

- Readily accessible, high-fidelity simulation tools to support training and exercises in incident management and response.

3.6 Emergency Services Sector National Preparedness Efforts

Due to the all-encompassing nature of the ESS mission, the sector's security and resilience strategies and activities cross the entire national preparedness spectrum of prevention, protection, mitigation, response, and recovery from an incident. Efforts to enhance the national preparedness mission areas translate to a more secure and resilient ESS and, therefore, a more secure and resilient Nation.

Numerous security and resilience programs and activities exist throughout the sector that involve measures designed to prevent, deter, and mitigate threats; reduce vulnerability to disasters; minimize consequences; and enable timely, efficient response and restoration following incidents and natural or manmade disasters. Every day across the United States, the ESS organizes and executes its security and resilience programs and activities in a manner consistent with all five of the national preparedness frameworks that correspond to the five mission areas—National Prevention Framework, National Protection Framework, National Mitigation Framework, National Response Framework, and National Disaster Recovery Framework—in addition to the implementation of the National Incident Management System. These programs and activities that contribute to the security and resilience of the sector are diverse and developed by numerous Federal and SLTT agencies, ESS discipline-specific trade associations, and education and training institutions that support the sector's specialized capabilities.

The scope of the ESS mission produces wide-ranging security and resilience activities that are uniquely tied to the responsibility to implement the 31 core capabilities that support the 5 national preparedness mission areas. These core capabilities are distinct critical elements required to achieve the goal of national preparedness and are present across many ESS activities.

Prevention

Prevention efforts are closely related to efforts that address threats and are reflected in ESS activities to conduct assessments, such as threat assessments. ESS examples include:

- Providing timely, accurate, and actionable information and exchanging information, data, and knowledge among Federal, SLTT, and private sector ESS entities, as appropriate.
- Leveraging the ESS-CRA and Roadmap to inform and direct cybersecurity preparedness efforts for the ESS, and other sectors by proxy.

- Strengthening community planning and preparedness for chemical facility assets through the activities identified in EO 13650.
- Assisting with the development of a training resource that lists specific chemical safety and security training courses for first responders and emergency planners.

Protection

Protection efforts generally address vulnerabilities, such as in ESS programs and activities that focus on assessing vulnerabilities and addressing those vulnerabilities. ESS examples include:

- Documenting and promulgating current credentialing and crisis reentry efforts, which support nationwide critical infrastructure resilience activities.
- Developing, through the ESS Working Group on Medical Countermeasures, a national strategy for protecting the health of emergency services personnel, thereby protecting the capacity of the ESS.
- Participating in efforts by EPA, DHS, OSHA, and the Bureau of Alcohol, Tobacco, Firearms, and Explosives to share information on chemical assets with first responders.

Mitigation

Mitigation efforts transcend all three components of understanding critical infrastructure risk—threat, vulnerability, and consequence. Mitigation covers a wide range of activities that include anything from planning activities to long-term vulnerability reduction activities. ESS examples include:

- Assessing risk to enable decision-makers and ESS stakeholders to take informed action to reduce risk to the sector and increase their resilience.
- Identifying the threats and hazards that may affect the ESS, determining the frequency and magnitude of impact, and incorporating this into planning processes to make informed risk management decisions.

Response

Response efforts are intimately tied to recovery efforts in that both help to minimize consequences. ESS examples include:

- Delivering search and rescue capabilities through ESS personnel, services, and assets.
- Ensuring a safe and secure environment through law enforcement and related security operations for locations affected by an incident, including for internal ESS disciplines.

Recovery

Recovery efforts include those activities that are necessary to assist affected locations in recovering effectively from an incident. While the ESS is not deeply involved in the recovery mission, a role exists for the sector in facilitating an environment of recovery and community resilience. ESS examples include:

- Restoring the health and social services networks to benefit the whole community.
- Ensuring communications among ESS, Federal, and SLTT entities continue to support information sharing and documenting lessons learned.

CHAPTER ENDNOTES

1. U.S. Department of Homeland Security (DHS) "Emergency Services Sector Cybersecurity Initiative," last modified June 10, 2014, www.dhs.gov/emergency-services-sector-cybersecurity-initiative.
2. U.S. Department of Homeland Security (DHS), "PCII Protections from Disclosure," last modified August 14, 2014, www.dhs.gov/pcii-protections-disclosure.

4 VISION, MISSION, GOALS, AND PRIORITIES

EMERGENCY SERVICES SECTOR VISION

An Emergency Services Sector in which personnel and operational capabilities are prepared for and resilient to inherent and unforeseen risks; ensuring timely, coordinated all-hazards emergency response and public confidence in the sector.

EMERGENCY SERVICES SECTOR MISSION

Save lives, protect property and the environment, assist communities impacted by disasters, and aid recovery during emergencies.

4.1 Goals and Priorities

The following ESS goals and priorities (which are equivalent to objectives in ESS planning) represent the sector's view of how best to support the five overarching goals of the NIPP 2013 and Joint National Priorities and to achieve a secure, protected, and resilient ESS. Emphasizing collaboration among all sector partners, the goals provide the framework to guide ESS security and resilience efforts, inform partner decisions, and improve risk management practices. The priorities (objectives) take into consideration the unique risk management perspectives and resources of the ESS, and focus on enduring capabilities that serve the sector's preparedness and protective needs over the long term, which promotes sustainability and resilience. A summary of how ESS goals and priorities contribute to the NIPP 2013 goals and Joint National Priorities is located in Appendix B.

Table 1. Emergency Services Sector Goals and Priorities

Goals		Priorities	
1	**PARTNERSHIP ENGAGEMENT** Continuous growth and improvement of sector partnerships, which enable the sector to effectively sustain collaborative dialogues to address risk mitigation and resilience efforts within the sector.	PRIORITY A	Utilize collaborative approaches to strengthen critical infrastructure protective planning and decision-making.
		PRIORITY B	Develop and refine processes and mechanisms for ongoing coordination and collaboration through councils and working groups that support development and implementation of protective programs.
		PRIORITY C	Enhance sector engagement models by identifying and partnering in like efforts focused on ESS issues.
2	**SITUATIONAL AWARENESS** Support an information-sharing environment that ensures the availability and flow of accurate, timely, and relevant sector information, intelligence, and incident reporting.	PRIORITY D	Collaborate with our partners to develop and share appropriate risk and capacity building information to support sector requirements.
		PRIORITY E	Enhance the sector's ability to share information through innovative processes and technologies.
		PRIORITY F	Identify sector information-sharing requirements for data, tools, and processes.

Goals		Priorities	
3	**PREVENTION, PREPAREDNESS, AND PROTECTION** Employ a risk-based approach to improve the preparedness and resilience of the sector's overall capacity to perform its mission through targeted decisions and initiatives.	PRIORITY G	Identify and implement an approach/process to assess and prioritize risk and capability gaps in the ESS.
		PRIORITY H	Collaborate and share ESS model practices and protective measures with sector partners.
		PRIORITY I	Develop and report metrics to measure effectiveness of sector efforts and gather a means to measure effectiveness.
4	**RECOVERY AND RECONSTITUTION** Improve the operational capacity sustainability and resilience of the sector and increase the speed and efficiency of restoration of normal services and activity following an incident.	PRIORITY J	Strengthen all components of an integrated region-wide response and recovery capability.
		PRIORITY K	Enhance the ability of Federal, State, local, tribal, and territorial governments and the private sector to recover effectively from crises resulting from a terrorist attack, natural disaster, or other incidents.
		PRIORITY L	Improve and expand effective resource sharing systems and standards.

4.2 Sector Activities

ESS partners developed a set of 18 activities that the sector can collaboratively conduct to effectively implement its SSP and meaningfully contribute to the sector goals and priorities. The following table presents collaborative, voluntary activities that sector GCC and SCC representatives will pursue with support and guidance from the SSA over the next 1-4 years. While the SSPs are updated every four years, the GCC and SCC will annually prioritize and develop a list of discrete, detailed tasks to pursue over the coming year, considering timing, available resources, and feasibility. During this time, the partnership may also update the activities to reflect evolving risk, changing resource allocations, and progress or completion.

Sector partners recognize that no individual entity has authority over resources and budgets for the entire ESS. Federal, SLTT, and private sector partners contribute funds, personnel, expertise, and other valuable resources to sector security and resilience activities. Considering that ESS partners operate in extremely limited resource environments and that security and resilience investments are becoming increasingly expensive, the ability to achieve each of the identified activities will depend on resources or funding allocations that are largely outside of the control of individual sector partners. In addition, current and future resource limitations may not allow for completion of all identified activities. Rather than constrain priorities and activities based on available funding alone, the sector identified the activities it believes will make a significant contribution to national security and resilience, which can be used to prioritize resources as they become available.

Table 2. Emergency Services Sector Activities Mapped to Sector Priorities

Map to Priority		Sector Activities
A	1	Collaborate with sector partners and stakeholders to promote the ESS-CRA, the Roadmap, and the Cyber Exercise Program. Inform and improve efforts in order to expand cybersecurity awareness and knowledge about sector-specific threats. Develop and implement a review process to update these initiatives.

Map to Priority		Sector Activities
B	2	Identify and promote effective public-private partnership practices, including evaluating ESS partnership participation to increase attendance and number of partnership activities.
C	3	Increase cross-sector collaboration and coordination on topics of importance to the ESS, such as access credentialing, mapping interdependencies, and issues in common with the lifeline sectors.
C	4	Collaborate with the IAB on issues and associated standards of common interest, such as sector planning, assessment tools, cybersecurity, training, and R&D.
C	5	Review and inform sector taxonomy to reflect the current sector landscape and growing member constituency.
D	6	Mature a resilience development-focused program of capacity-building products and expertise focused on the unique needs of the sector. Offer the program to ESS practitioner organizations to provide customized enhancements to their resilience and overall readiness.
D	7	Engage with local emergency planning organizations, such as Local Emergency Planning Committees, to enhance information sharing and analytical capabilities for incident planning, management, and mitigation between ESS stakeholders.
E	8	Define, map, prioritize, and assess the effectiveness of ESS information-sharing requirements, sources, types, and mechanisms. Conduct exercises to examine the mechanisms and test the capabilities of public and private sector partners.
E	9	Develop a process to incorporate information from multiple and nontraditional sources (e.g., crowdsourcing and social media) into incident command operations and share the process with sector partners.
F	10	Develop and approve ESS-focused Standing Information Needs to assist the intelligence community with identifying and building threat-related materials.
G	11	Develop ESS-specific resources based on stakeholder requirements for self-assessment of operational risks, capability gaps, and response capacity.
G	12	Develop a sector-wide risk assessment to serve as a roadmap for defining capability gaps within the sector and guide future partnership efforts.
H	13	Develop a summary explaining the benefits of ESS utilization of the NIST Framework for Improving Critical Infrastructure Cybersecurity.
H	14	Identify readily accessible, high-fidelity simulation tools to support training and exercises in incident management and response.
I	15	Identify existing sector partnership metrics that are effective in sustaining and enhancing the partnership.
J	16	Develop and implement a strategy to educate public and private emergency responders on—and increase their use of—the JSOP/ER-ITN for crisis reentry and access control.
K	17	Implement a process for reviewing after-action reports (e.g., from sector exercises, local and national incidents, and other collaborative engagements); define capability gaps and develop appropriate activities to address the gaps.
L	18	Identify requirements for monitoring, in real time, the status of sector resources and their functionality and availability in extreme conditions.

5 MEASURING EFFECTIVENESS

Performance measurement efforts are an important step in determining the effectiveness of risk management investments, programs, and activities. Individual ESS partners use a variety of indicators to measure the efficacy and continuous improvement of their security and resilience risk management processes. Measuring improvements in security and resilience at the sector level is far more difficult. Where possible, sector partners attempt to measure how their voluntary partnership activities contribute to risk reduction and enhanced resilience across the sector without precluding or impinging the measurement efforts of individual sector partners.

As the SSA, DHS has the primary responsibility for measuring and reporting progress toward sector activities using relevant metrics. An established performance metrics system designed to track the progress of sector activities is used to ensure accurate and consistent measurement.

Table 3 aligns ESS activities with a set of possible performance metrics that the SSA may use to measure and report progress, where possible. The metrics not only measure the completion of the activity—using output measures such as the number of products developed or partners engaged—but also aim to measure the outcomes of these activities—particularly how effective they are in achieving progress toward sector goals.

Within the voluntary sector partnership, often the best available outcome measure is to track intent to act based on the information, tools, or guidance received through sector activities. The SSA measures this intent to act using a survey—during or following each engagement or activity—that asks three things:

- Was the information received current and relevant?
- Will the information inform decision-making?
- Will participants further share the information within their organization?

Survey results indicate the effectiveness of each activity in equipping participants with the information, tools, guidance, and processes to take actions that ultimately reduce or better manage sector risk.

The SSA will report sector progress through the National Annual Report and the quadrennial SSP updates. The following list is not exhaustive of all possible ways to measure effectiveness, and sector partners may voluntarily measure and report additional information on sector progress during the National Annual Reporting process.

Table 3. Emergency Services Sector Activities and Expected Metrics

	Emergency Services Sector Activities	Expected Metrics
1	Collaborate with sector partners and stakeholders to promote the ESS-CRA, the Roadmap, and the Cyber Exercise Program. Inform and improve efforts in order to expand cybersecurity awareness and knowledge about sector-specific threats. Develop and implement a review process to update these initiatives.	• Information products developed to promote cybersecurity awareness and sector-specific threats • Number of meetings and workshops organized or coordinated with sector partners to promote the cybersecurity awareness and sector-specific threat and level of participation over time • How participants and recipients intend to use the information provided • Status of developing a review process to update initiatives
2	Identify and promote effective public-private partnership practices, including evaluating ESS partnership participation to increase attendance and number of partnership activities.	• Number of meetings and workshops organized or coordinated with sector partners to identify and promote public-private partnership practices and level of participation over time • How participants intend to use the information provided

	Emergency Services Sector Activities	Expected Metrics
3	Increase cross-sector collaboration and coordination on topics of importance to the ESS, such as access credentialing, mapping interdependencies, and issues in common with the lifeline sectors.	• Number of meetings and workshops organized or coordinated with other sectors and level of participation over time • How participants intend to use the information provided
4	Collaborate with the IAB on issues and associated standards of common interest, such as sector planning, assessment tools, cybersecurity, training, and R&D.	• Number of meetings and workshops organized or coordinated with the IAB and level of participation over time • Number of products or activities completed by the IAB to support sector resilience
5	Review and inform sector taxonomy to reflect the current sector landscape and growing member constituency.	• Status of reviewing sector taxonomy
6	Mature a resilience development-focused program of capacity-building products and expertise focused on the unique needs of the sector. Offer the program to ESS practitioner organizations to provide customized enhancements to their resilience and overall readiness.	• Products developed and their distribution • How recipients intend to use the information provided
7	Engage with local emergency planning organizations, such as Local Emergency Planning Committees, to enhance information sharing and analytical capabilities for incident planning, management, and mitigation between ESS stakeholders.	• Number of meetings and workshops organized or coordinated with local-level emergency planning organizations and level of participation over time • How participants intend to use the information provided
8	Define, map, prioritize, and assess the effectiveness of ESS information-sharing requirements, sources, types, and mechanisms. Conduct exercises to examine the mechanisms and test the capabilities of public and private sector partners.	• Status of information-sharing assessments • Number of exercises organized or coordinated to test information-sharing mechanisms • How participants intend to use the information provided
9	Develop a process to incorporate information from multiple and nontraditional sources (e.g., crowdsourcing and social media) into incident command operations and share the process with sector partners.	• Status of process development • Once complete, measure dissemination and use
10	Develop and approve ESS-focused Standing Information Needs to assist the intelligence community with identifying and building threat-related materials.	• Status of development/review of ESS-focused Standing Information Needs (biannual) • Products developed and their distribution • How recipients intend to use the information provided
11	Develop ESS-specific resources based on stakeholder requirements for self-assessment of operational risks, capability gaps, and response capacity.	• Status of ESS-specific resources development • Products developed and their distribution • How recipients intend to use the information provided

	Emergency Services Sector Activities	Expected Metrics
12	Develop a sector-wide risk assessment to serve as a roadmap for defining capability gaps within the sector and guide future partnership efforts.	• Status of developing sector-wide risk assessment • Products developed based on the assessment and their distribution • How recipients intend to use the information provided
13	Develop a summary explaining the benefits of ESS utilization of the NIST Framework for Improving Critical Infrastructure Cybersecurity.	• Status of summary development • Products developed and their distribution • How recipients intend to use the information provided
14	Identify readily accessible, high-fidelity simulation tools to support training and exercises in incident management and response.	• Number of meetings and workshops organized or coordinated with stakeholders to identify tools and level of participation over time • Products developed and their distribution • How participants and recipients intend to use the information provided
15	Identify existing sector partnership metrics that are effective in sustaining and enhancing the partnership.	• Number of meetings and workshops organized or coordinated with sector partners to identify existing sector partnership metrics and level of participation over time • Effective partnership metrics identified or developed • How participants intend to use the information provided
16	Develop and implement a strategy to educate public and private emergency responders on—and increase their use of—the JSOP/ER-ITN for crisis reentry and access control.	• Status of developing and implementing a strategy • Number of meetings and workshops organized or coordinated with stakeholders to implement a strategy and level of participation over time • Products developed and their distribution • Number of ER-ITN participants
17	Implement a process for reviewing after-action reports (e.g., from sector exercises, local and national incidents, and other collaborative engagements); define capability gaps and develop appropriate activities to address the gaps.	• Status of process implementation • Number of meetings and workshops organized or coordinated with stakeholders to define capability gaps and develop appropriate activities and level of participation over time • Products developed and their distribution • How participants and recipients intend to use the information provided
18	Identify requirements for monitoring, in real time, the status of sector resources and their functionality and availability in extreme conditions.	• Status of identifying requirements. • Number of meetings and workshops organized or coordinated with stakeholders to identify requirements and level of participation over time • Products developed and their distribution • How participants and recipients intend to use the information provided

APPENDIX A
Acronyms and Terms

AOR	area of responsibility
CARMA	Cybersecurity Assessment and Risk Management Approach
CARVER	Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability
CBRN	chemical, biological, radiological, or nuclear
CDRWG	Credentialing and Disaster Reentry Working Group
CISR	critical infrastructure security and resilience
COOP	continuity of operations
CS&C	Office of Cybersecurity and Communications
DHS	U.S. Department of Homeland Security
ECIP	Enhanced Critical Infrastructure Protection
EMR-ISAC	Emergency Management and Response—Information Sharing and Analysis Center
EMS	emergency medical services
EO	Executive Order
EOC	Emergency Operations Center
EPA	U.S. Environmental Protection Agency
ER-ITN	Emergency Responder Identity Trust Network
ES	Emergency Services
ESS	Emergency Services Sector
ESS-CRA	*Emergency Services Sector-Cyber Risk Assessment*
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FRG	First Responders Group
FRRG	First Responder Resource Group
GCC	Government Coordinating Council
HazMat	Hazardous Materials
HIRA	Hazard Identification and Risk Assessment
HSIN	Homeland Security Information Network
HSIN-ES	Homeland Security Information Network-Emergency Services
IAB	InterAgency Board
IED	improvised explosive device
IP	Office of Infrastructure Protection
IT	information technology
JSOP	Crisis Reentry Joint Standard Operating Procedure
LEPC	Local Emergency Planning Committee
NCCAD	National Counter-IED Capabilities Asset Database
NIPP 2013	*National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience*
NIST	National Institute of Standards and Technology
OSHA	Occupational Safety and Health Administration
PR3	Project Responder 3
PR4	Project Responder 4
PSA	Protective Security Advisor
R&D	Research and Development
Roadmap	*Emergency Services Sector Roadmap to Secure Voice and Data Systems*
S&T	Science and Technology Directorate
SAR	search and rescue
SCC	Sector Coordinating Council
SLTT	State, local, tribal, and territorial
SSA	Sector-Specific Agency
SSP	Sector-Specific Plan
SWAT	Special Weapons and Tactics
THIRA	Threat and Hazard Identification and Risk Assessment
TRIP*wire*	Technical Resource for Incident Prevention
US-CERT	United States Computer Emergency Readiness Team
USFA	United States Fire Administration

APPENDIX B
Alignment with the NIPP 2013

Table B-1. Emergency Services Sector Priorities Aligned with Joint National Priorities and NIPP 2013 Goals

Emergency Services Sector Priorities	Joint National Priorities					NIPP 2013 Goals				
	Strengthen Management of Cyber and Physical Risks to Critical Infrastructure	Build Capabilities and Coordination for Enhanced Incident Response and Recovery	Strengthen Collaboration Across Sectors, Jurisdictions, and Disciplines	Enhance Effectiveness in Resilience Decision-making	Share Information to Improve Prevention, Protection, Mitigation, Response, and Recovery Activities	1	2	3	4	5
A Collaborate to strengthen planning	PRIORITY A		PRIORITY A	PRIORITY A				X		
B Refine coordination process			PRIORITY B	PRIORITY B				X		
C Enhance engagement models			PRIORITY C					X		
D Develop and share risk and capacity information	PRIORITY D	PRIORITY D	PRIORITY D		PRIORITY D				X	
E Innovate information-sharing processes		PRIORITY E	PRIORITY E		PRIORITY E				X	
F Identify information-sharing requirements	PRIORITY F				PRIORITY F				X	
G Identify and implement risk assessment and prioritization	PRIORITY G			PRIORITY G		X				
H Collaborate and share model practices	PRIORITY H	PRIORITY H	PRIORITY H		PRIORITY H					X
I Develop and report metrics	PRIORITY I			PRIORITY I						X
J Strengthen region-wide response and recovery		PRIORITY J	PRIORITY J		PRIORITY J		X			
K Enhance government and private sector recovery		PRIORITY K	PRIORITY K		PRIORITY K		X			
L Improve and expand resource sharing		PRIORITY L	PRIORITY L	PRIORITY L	PRIORITY L		X			

NIPP 2013 Goals

1. Assess and analyze threats to, vulnerabilities of, and consequences to critical infrastructure to inform risk management activities.
2. Secure critical infrastructure against human, physical, and cyber threats through sustainable efforts to reduce risk, while accounting for the costs and benefits of security investments.
3. Enhance critical infrastructure resilience by minimizing the adverse consequences of incidents through advance planning and mitigation efforts and employing effective responses to save lives and ensure the rapid recovery of essential services.
4. Share actionable and relevant information across the critical infrastructure community to build awareness and enable risk-informed decision-making.
5. Promote learning and adaptation during and after exercises and incidents.

Table B-2. Contribution of the Emergency Services Sector Activities to the NIPP 2013 Calls to Action

	Emergency Services Sector (ESS) Contribution or Aligned Activity	NIPP 2013 Calls to Action											
		#1	#2	#3	#4	#5	#6	#7	#8	#9	#10	#11	#12
1	Collaborate with sector stakeholders and partners to promote the ESS-CRA, the Roadmap, and the Cyber Exercise Program. Inform and improve efforts in order to expand cybersecurity awareness and knowledge about sector-specific threats. Develop and implement a review process to update these initiatives.		X							X			
2	Identify and promote effective public-private partnership practices, including evaluating ESS partnership participation to increase attendance and number of partnership activities.		X	X	X					X		X	
3	Increase cross-sector collaboration and coordination on topics of importance to the ESS, such as access credentialing, mapping interdependencies, and issues in common with the lifeline sectors.		X				X	X	X	X			
4	Collaborate with the InterAgency Board on issues of common interest, such as sector planning, assessment tools, cybersecurity, training, and R&D.		X							X	X		
5	Review and inform sector taxonomy to reflect the current sector landscape and growing member constituency.					X							
6	Mature a resilience development-focused program of capacity-building products and expertise focused on the unique needs of the sector. Offer the program to ESS practitioner organizations to provide customized enhancements to their resilience and overall readiness.				X	X				X			
7	Engage with local emergency planning organizations, such as Local Emergency Planning Committees, to enhance information sharing and analytical capabilities for incident planning, management, and mitigation between ESS stakeholders.					X		X	X				
8	Define, map, prioritize, and assess the effectiveness of ESS information-sharing requirements, sources, types, and mechanisms. Conduct exercises to examine the mechanisms and test the capabilities of public and private sector partners.					X				X			X
9	Develop a process to incorporate information from multiple and nontraditional sources (e.g., crowdsourcing and social media) into incident command operations.					X				X	X		
10	Develop and approve ESS-focused Standing Information Needs to assist the intelligence community with identifying and building threat-related materials.					X							
11	Develop ESS sector-specific resources, based on stakeholder requirements, for self-assessment of capability gaps, operational and capacity risks, and analytical needs.		X	X		X		X					
12	Develop a sector-wide risk assessment to serve as a roadmap for defining capability gaps within the sector and guide future partnership efforts.		X	X		X		X					
13	Develop a summary explaining the benefits of ESS utilization of the NIST Framework for Improving Critical Infrastructure Cybersecurity.				X					X			
14	Identify readily accessible, high-fidelity simulation tools to support training and exercises in incident management and response.					X				X	X		
15	Identify existing partnership metrics that are effective to sustain and enhance the partnership.											X	
16	Develop and implement a strategy to educate public and private sector emergency responders on—and increase their use of—the JSOP/ER-ITN for crisis reentry and access control.								X	X	X		

	Emergency Services Sector (ESS) Contribution or Aligned Activity	NIPP 2013 Calls to Action											
		#1	#2	#3	#4	#5	#6	#7	#8	#9	#10	#11	#12
17	Implement a process for reviewing after-action reports (e.g., from sector exercises, local and national incidents, and other collaborative engagements); define capability gaps and develop appropriate activities to address the gaps.								X				X
18	Identify requirements for monitoring, in real time, the status of sector resources and their functionality and availability in extreme conditions.					X							
	Emergency Services Sector goals and priorities were developed in alignment with the 2014 Joint National Priorities in support of Call to Action #1.	X											
	Development of the 2015 Emergency Services Sector-Specific Plan meets Call to Action #2.		X										
	The Emergency Services Sector supports Call to Action #10 by working with its Federal partners to implement the *National Critical Infrastructure Security and Resilience Research and Development Plan*.										X		
	The measurement approach outlined in Chapter 5: Measuring Effectiveness will enable the Emergency Services Sector to evaluate and report on the progress of partnership efforts in support of Call to Action #11.											X	

NIPP 2013 Calls to Action

Call to Action #1: Set National Focus through Jointly Developed Priorities

Call to Action #2: Determine Collective Actions through Joint Planning Efforts

Call to Action #3: Empower Local and Regional Partnerships to Build Capacity Nationally

Call to Action #4: Leverage Incentives to Advance Security and Resilience

Call to Action #5: Enable Risk-Informed Decision-making through Enhanced Situational Awareness

Call to Action #6: Analyze Infrastructure Dependencies, Interdependencies, and Associated Cascading Effects

Call to Action #7: Identify, Assess, and Respond to Unanticipated Infrastructure Cascading Effects During and Following Incidents

Call to Action #8: Promote Infrastructure, Community, and Regional Recovery Following Incidents

Call to Action #9: Strengthen Coordinated Development and Delivery of Technical Assistance, Training, and Education

Call to Action #10: Improve Critical Infrastructure Security and Resilience by Advancing Research and Development Solutions

Call to Action #11: Evaluate Progress Toward the Achievement of Goals

Call to Action #12: Learn and Adapt During and After Exercises and Incidents

Homeland
Security