C

Critical Infrastructure: Emergency Services Sector

Brian Keith Simpkins
Homeland Security Program, Eastern Kentucky University, Richmond, KY, USA

Keywords
Dependencies · First Responder · Interdependencies · Natural Hazards · Risk Profile

Definitions

Critical Infrastructure: “Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters” (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism [USA PATRIOT] Act 2001).

Emergency Services Sector: The Emergency Services Sector (ESS) provides services to all five mission areas defined in the National Preparedness Goal: prevention, protection, mitigation, response, and recovery (U.S. Department of Homeland Security [DHS] 2015c). The services are provided by career and volunteer first responders and associated capabilities and resources across the county at the federal, state, and local levels as well as the private sector (U.S. Department of Homeland Security [DHS] 2015a).

Introduction

Each and every day, the Emergency Services Sector (ESS) plays an important role in safeguarding lives and property across the United States. Although the ESS responds when assets in other critical infrastructure sectors need assistance, the sector itself faces challenges to security and resilience. Some of the risks faced by the ESS are similar to other infrastructure sectors, such as a changing threat and hazard picture, climate change, and cyber-attacks through increased reliance on Internet-connected systems. These high-level challenges are just the beginning as the ESS faces a myriad of other risks related to natural hazards, technological hazards, and

L. R. Shapiro, M-H. Maras (eds.), *Encyclopedia of Security and Emergency Management*,
https://doi.org/10.1007/978-3-319-69891-5_62-1

human-caused incidents. This is in addition to dependencies and interdependencies with other infrastructure sectors, which can result in significant cascading effects.

The remainder of this entry provides a general overview of the ESS to enable a general understanding. Within the discussion, key operational characteristics of the ESS are reviewed along with a description of the current risk profile to include critical cross-sector dependencies and interdependencies. This discussion will also include vision/mission, goals, and priorities of the ESS along with the partnership structure. Partnerships and information sharing within the ESS have extreme importance in order to address and respond to human-caused incidents that can result in significant casualties and damage to infrastructure assets. Overall, this entry provides a basic understanding of the ESS to enable critical evaluation of current policies, practices, and needed activities to address gaps in security and resilience.

Sector Overview

The ESS has the primary protection responsibility of other critical infrastructure sectors and assets. The ESS is the first line of defense for all mission areas (prevention, protection, response, recovery, and mitigation) related to natural hazards, technological hazards, and human-caused incidents that may affect infrastructure assets. To accomplish this task, the ESS consists of millions of highly skilled first responders (human element) along with physical and cyber assets/elements. Consisting of both paid and volunteer forces, the ESS is organized/structured at the federal, state, local, tribal, and territorial levels of government. Therefore, ESS agencies include the primary public first responder agencies at each government level. ESS assets also include personnel and associated resources within the private sector such as private security and fire/emergency medical services at industrial sites. Due to the focus on the protection of other infrastructure sectors and assets, the ESS faces distinctive challenges in security and resilience of ESS assets, such as communications and data networks. The disruption of physical or virtual ESS assets can result in significant consequences to public safety and security.

Sector Components and Assets

The ESS has components related to the human, physical, and cyber elements. For human, the ESS is comprised of paid and volunteer individuals within the primary response disciplines. For physical, this realm includes ESS facilities from which daily operations are administered as well as facilities that support training and storage. Additional physical assets include equipment (e.g., personal protective [PPE], communications, and surveillance equipment) and vehicles (e.g., ambulances, patrol vehicles, fire apparatus, aircraft, and watercraft) that are specialized for specific disciplines and for capability. In regard to cyber, this element includes operational communications (e.g., two-way radio systems), databases (e.g., criminal record databases), management (e.g., incident decision support software), biometric systems, security systems, and information networks (e.g., computer-aided dispatch [CAD]). Aside from human, physical, and cyber realm, the ESS is officially compartmentalized into five distinct emergency responder disciplines or subsectors as described below per the *Emergency Services Sector-Specific Plan* (ES SSP).

Law Enforcement: Consists of police departments, sheriff's offices, courts systems, correctional institutions, and private security agencies. Provides services such as enforcing laws, conducting criminal investigations, collecting evidence, apprehending suspects, securing the judicial system, and ensuring custody and rehabilitation of offenders.

Fire and Rescue Services: Consists of both paid and volunteer personnel. Provides services such as fire suppression, fire prevention, hazardous materials control, life and property safety operations (including technical rescue), building code enforcement, and fire safety education.

Emergency Medical Services: Provides services at incidents such as 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.

Emergency Management: Provides incident management and coordination (including pre- and postevent activities) between ESS disciplines, as well as with nonemergency services entities. Emergency Operations Centers (EOCs) provide emergency management personnel with the capability for multiagency coordination for incident management by activating and operating for preplanned or no-notice events. EOCs support the coordination of response and recovery activities among neighboring jurisdictions at and all levels of government if needed.

Public Works: Provides service 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 (U.S. Department of Homeland Security [DHS] 2015a, p. 5).

In addition to the responder disciplines/subsectors, the ESS also consists of specialized personnel and teams that provide additional emergency response capability when appropriate. This specialized capability can be present in one or more of the responder disciplines/subsectors and can focus in areas such as special weapons and tactics, hazardous materials, explosive ordinance disposal, search and rescues (air, land, marine), and National Guard Civil Support (DHS 2015a).

Key Sector Operating Characteristics

As previously stated, the ESS has the primary protection responsibility of other critical infrastructure sectors and assets and acts as the first line of defense in relation to natural hazards, technological hazards, and human-caused incidents that may affect infrastructure assets. This responsibility is handled by more than 2.5 million first responders that serve in all 56 US states and territories (DHS 2015a). Decisions made by the ESS in response to incidents can affect the level of damage inflicted to infrastructure and how quickly services are restored. Although the ESS operations are required to be adaptable and flexible to address any incident, the sector does have limitations when facing incidents and disasters – or circumstances – which have not been training for or previously experienced. Overall, the graphically dispersed aspect of the ESS makes it difficult to completely disable nationwide, but this aspect also creates challenges in across government levels and responder disciplines. Further, the ESS is driven by the human element, but is dependent on the cyber element (e.g., communications, information technology) and physical element (e.g., response vehicles and equipment).

Another limitation of the ESS is limited resources, especially in ESS agencies located in small and rural communities. Not only have operational budgets within local and state ESS agencies decreased over the past decade, but federal grant funding for ESS agencies has also vastly decreased over the same time period. Limited financial budgets affect the operational capacity of ESS agencies (e.g., less personnel, use of older/outdated equipment) to address and respond to current risks and adapt to changing risks. Resource constraints are just one operational consideration of the ESS, and others include the following:

Rural and Frontier Resource Constraints: In rural and frontier communities, limited populations and smaller tax bases create difficulties and shortcomings for ESS agencies in terms of staffing, equipment, and other resources.

Geography: The ESS operates in density-populated urban environments as well as in vast and, oftentimes, sparsely populated areas, both of which provide significant challenges. For example, in rural and frontier areas, greater distances traveled and difficult on-road and off-road terrain (e.g., mountains, marshlands, wilderness) may significantly impact response planning and operations.

Infrastructure: Although urban ESS agencies may benefit operationally from an increased presence of infrastructure, it also creates more infrastructure to protect. As for rural areas, many segments of critical infrastructure, such as hospitals and other healthcare facilities, are less capable (e.g., have fewer physicians and specialists per capita) than similar infrastructure in urban areas for various reasons. These conditions may limit response to public health hazards such as communicable diseases.

Modernization: Citizens of all communities continue to demand that ESS agencies modernize systems despite resource shortages. Today, approximately 88% of US adults own a cell phone and 78% access the Internet. ESS agencies must upgrade their own equipment as well as 9-1-1 centers, warning systems, and online resources for the benefit of their residents (Simpkins 2015, p. 3).

All of the constraints above are intensified by the fact that a majority of ESS personnel are volunteers. For example, volunteers are often assigned as county emergency managers and/or required to fully staff rural fire departments (U.S. Fire Administration 2007). This occurrence does not happen in rare circumstances. Rather, rural areas constitute 80% of the landmass and 20% of the population in the United States (McGinnis 2004). Additionally, frontier areas are classified as areas with an extremely low population density (less than six persons per square mile) and are characterized by isolation from population centers (e.g., cities) and provision of services (e.g., hospital, cell phone service), which comprise approximately 2% of the US population and 46.7% of the land within the Unites States (largely concentrated in the Western United States and Alaska) (National Center for Frontier Communities 2013).

Across the United States, ESS missions are completed by approximately 2.6 million individuals in the law enforcement, fire and rescue, emergency medical services (EMS), emergency management, and public works disciplines (DHS 2015a). This is in addition to ESS personnel within the private sector that includes industrial fire departments, corporate security operations, and private EMS providers. As for the number of rural first responders, there is no single source for a specific number. However, descriptive information can be gleaned from various sources. For example, the National Institute of Justice (2004) reports that approximately 90% (or ~14,500) of the over 16,000 municipal and county law enforcement agencies in the United States serve populations under 25,000 and over half of all agencies employ 10 or fewer officers. Further, the US Fire Administration (2007) reports that 44% (or ~13,440) of the over 30,000 fire departments in the United States are located in rural areas.

Similar to other critical infrastructure sectors, the ESS is not heavily regulated, but specific regulations govern or provide reference for use in emergency response operations (e.g., hazardous materials incidents), responder safety (through the Occupational Safety and Health Administration [OSHA], and professional codes and standards for fire prevention and public safety (through the National Fire Prevention Association [NFPA]). Despite limited regulation, the agencies across the ESS rely heavily on communications and information technology networks during incident response. Protecting these networks is essential for ESS agencies to support critical infrastructure security and resilience as well as to ensure the provision or quick restoration of essential public services and infrastructure assets.

Sector-Specific Agency

The US government by itself cannot create a secure and resilient ESS. Rather, the end goal requires a dedicated whole-of-nation approach involving public and private stakeholders. Leading this whole-of-nation approach is the designated Sector-Specific Agency (SSA) as defined in *Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience*. The designated SSA for the ESS is DHS. More specifically, the Office of Infrastructure Protection is the delegated responsible entity within DHS.

Sector Partnerships

Security and resilience of the ESS requires a broad spectrum of partnerships to facilitate information sharing and situational awareness to address sector risks. Specific partnership structures are defined within the ES SSP. However, the ESS utilizes the *National Infrastructure Protection Plan* (NIPP) partnership structure and additional collaboration mechanisms based on Government Coordinating Councils (GCC) and the Sector Coordinating Councils (SCC). Beginning with the SCCs, these councils are comprised of owners and operators who utilize the council to directly collaborate with one another. Typically organized under subsectors within an overall infrastructure sector, SCCs are self-organized, self-run, and self-governed councils and serve as principal collaboration points between the GCCs and the SSAs. Conversely, the GCC focuses on collaboration and information sharing between the SSA, or federal departments and agencies, and state, local, tribal, and territory (SLTT) agencies. Members of the GCC and the SCC utilize collaborative mechanisms, such as the Critical Infrastructure Partnership Advisory Council (CIPAC) to facilitate collaboration and information sharing across the public and private sectors. These collaborative partnerships and subsequent information sharing are crucial to achieving infrastructure security and resilience. This enables public and private entities to freely share information to identify mutual risks and potential solutions that benefit entire sectors. Through the defined partnership structures of the ESS, overall security and resilience posture of the sector can be continuously improved.

Sector Risks

Despite the diverse collection of assets within the ESS, common risks exist that the sector must address. Climate change, extreme weather, terrorism, and malicious actors are persistent risks across the ESS (DHS 2014). Further, cyber vulnerabilities continue to increase as reliance on networked systems continues to rise in an effort to increase efficiency and cost-effectiveness. Some of these threats are more pronounced in the ESS due to the need for open public access and the responsibility to respond to any incident. This illustrates the need to comprehensively examine risks across the ESS through existing partnership structures in an effort to ensure security and resilience. Although numerous risks can be discussed, the following sections focus on those risks deemed significant. It is acknowledged there are other significant risks to the ESS, such as the loss of two-way communications. However, these risks will not be discussed for the sake of brevity. Expanded information on risks to the ESS is accessible via the ES SSP.

Cyber Risks

The cyber threat is common throughout all critical infrastructure sectors including the ESS. Information networks and other technology resources are vulnerable to various types of attacks, which continue to increase in occurrence and severity thereby resulting in significant risk to the ESS (DHS 2012, 2015b; U.S. Government Accountability Office [GAO] 2008, 2014; Green 2016). In fact, the cyber threat is considered one of the most serious threats to all critical infrastructure sectors. Like other infrastructure sectors, the ESS is heavily dependent on cyber infrastructure and operates in a data-driven environment. Further, much of the cyber infrastructure utilizes commercial-off-the-shelf (COTS) products and systems, which have inherent vulnerabilities to malicious individuals. Individuals both inside and outside of the United States attempt to exploit the vulnerabilities, which puts current and future

ESS capabilities at risk. In fact, the US Department of Defense (2011) *Strategy for Operating in Cyberspace* predicts the risk from foreign entities and non-state actors attempting to exploit cyber vulnerabilities will continue to increase in the future.

Ultimately, cyber vulnerability also poses a significant threat to the ESS sector and its ability to fight crime and complete other essential missions related to public safety and security. Most importantly is the ability to communicate, including the ability for citizens to reach ESS agencies via 9-1-1 services. More than just call centers, public-safety answering points (PSAPs) utilize information technology systems that merge phone numbers with geographic and other location data. These systems are vulnerable due to the increasing reliance on the Internet for operations, which makes 9-1-1 services susceptible to cyber-attacks. It is expected that attacks on ESS communication networks will become more frequent in the future (DHS 2015b; Green 2016). Between 2013 and 2016, over 600 critical government phone systems and 200 PSAPs nationwide were affected by telephony denial of service attacks (Green 2016). In addition to communications, the ESS is increasingly reliant on other cyber-based infrastructure for data and information management (including cloud-based systems), biometric activities, electronic security systems, and geospatial tools. Due to this connectivity, ESS cyber infrastructure is vulnerable to cyber-attacks (e.g., denial-of-service attacks, phishing, passive wiretapping, Trojan horses, viruses, worms) from individuals and group operating around the world (DHS 2015b; GAO 2014; Green 2016).

Another common threat to all computers and networks is ransomware, which encrypts or otherwise disables access to information unless a ransom is paid (a common form of payment requested is Bitcoin). The ESS is vulnerable to this threat as illustrated by multiple ESS agencies being targets of ransomware attacks since 2014 in states such as California, Nevada, Wisconsin, and North Carolina. These attacks can disrupt initial response by ESS agencies to an incident as well as endanger first responders and members of the general public. Ultimately, the ESS is increasingly dependent upon information technology networks for multiple operations, which greatly amplifies vulnerability to cyber-related incidents.

Climate Change, Natural Hazards, and Extreme Weather

As with other infrastructure sectors, the ESS is impacted by climate change. Not only are climate change risks present; their rate of occurrence and level of severity are increasing including their effects on natural hazards. Regardless of the natural hazard/disaster or extreme weather event, the ESS is faced with sometimes unpredictable natural threats in a dynamic response environment. Increased occurrence and severity of natural hazards place increased demands on ESS assets and threaten the provision of key services. These events are increasing in terms of geographic magnitude and severity thereby requiring a surge of ESS assets for extended operational periods. A recent example is the catastrophic flooding in the Houston (TX) due to Hurricane Harvey in late August 2017. In addition to ESS response personnel, natural hazards can also impact cyber infrastructure. This impact can be significant as 9-1-1 communication networks can be disrupted. Further, impacts from natural hazards can also impact ESS operational communications networks, such as two-ways radio communications.

Two events illustrate the risk from natural hazards to 9-1-1 communication systems and operational communications networks. First, a major storm during June 2012 resulted in a total disruption of telephone services supporting 9-1-1 service across several cities and counties in Virginia (GAO 2014). The service outage was a result of loss of main commercial power and subsequent failure of a backup generator in the telephone service provider's facilities (GAO 2014). The lack of redundant measures and mitigation planning contributed to a significant disruption of public service answering points (PSAP) operations during the outage (GAO 2014). Second, Hurricane Katrina resulted in the destruction or degradation of three million landlines, 2,000 cell towers, more than 30 public service answering points (PSAPs), 37 of 41 broadcast radio stations, and first responder land mobile radio service across the region (Miller 2006; Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina 2006). Satellite phones were in short supply and unable to be charged due to lack of electrical power and fuel to run emergency generators (Miller 2006; Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina 2006). The New Orleans (LA) Police Department and the Mississippi National Guard were unable to establish effective communications for several days (Miller 2006; Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina 2006). In addition to operable communication, situational awareness was nonexistent due to a lack of interoperability between federal, state, and local communications systems (Miller 2006; Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina 2006). This illustrates that the continued increase in the occurrence and severity of natural hazards will place demands on the ESS to mitigate operational disruptions while addressing increased public demand for service.

Epidemics and Pandemics

Evolving threats to the ESS include infectious disease occurrences, which can include diseases such as Ebola, smallpox, tuberculosis, severe acute respiratory syndrome (SARS), and Middle East respiratory syndrome (MERS) (National Infrastructure Advisory Council 2007). Infectious diseases can spread easily in today's highly mobile society and can easily morph into an epidemic (affecting a localized area) or pandemic (affecting a large region) (National Infrastructure Advisory Council 2007). A critical impact of an epidemic or pandemic is the loss of ESS personnel due to infections. Therefore, emerging and re-emerging infectious diseases must be planned for as ESS personnel would be important response assets. However, variation is persistent across the nation in terms of community fiscal health, at-risk population levels, training competencies, and countermeasure availability when addressing infectious disease epidemics and pandemics. These events can also have significant, long-term impacts on communities, especially in relation to high-risk and vulnerable populations. In fact, the United States has a constant risk of an onset of a severe influenza pandemic, and the influenza season of 2014 provides insight into the risk and how a rapidly spreading infectious disease can impact the ESS. A more concerning thought, however, is the intentional release of a more dangerous infectious disease such as smallpox and the catastrophic impacts on the nation if its spread is not readily contained.

Terrorism, Violent Extremism, and Malicious Actors

Due to the nature of their work, ESS personnel are vulnerable to human-caused incidents to include terrorism and actions by malicious actors to include active shooters. This is especially true for the ESS which perpetually faces the challenge to prepare for current threats as well as evolving threats that may require new or expanded capabilities and competencies. Further, response personnel can become targets of (secondary) attacks when responding to human-caused events in which an attacker's goal is to achieve a maximum amount of casualties. This is especially true if adversaries are targeting persons in specific authority positions or are symbolic of a social institution. Adversaries can include terrorists and violent extremists, who often target ESS personnel and symbolic targets.

Improvised Explosive Devices

The use of improvised explosive devices (IEDs) continues to be a common asymmetrical attack method by terrorists and violent extremists. Not only can IEDs damage infrastructure and cause mass causalities; they can also be used to target ESS personnel when responding to an initial incident through secondary devices. Another common practice is the simultaneous use of IEDs at multiple locations, which is specifically designed to affect ESS agency response efforts. Further, active shooter events can incorporate IEDs in an effort to increase causalities or hamper and slow down response from ESS agencies. For example, the perpetrators of the San Bernardino

(CA) shooting on December 2, 2015 placed a pipe bomb in the Inland Regional Center, but was not detonated (Winton and Queally 2016). Overall, the threat of IEDs is constant across many infrastructure sectors, including the ESS.

Primary Sector Dependencies and Interdependencies

Today, critical infrastructure sectors are highly dependent and interdependent on one another through physical and cyber linkages. After a natural disaster, man-made incident, or technological accident, a significant failure in one sector – such as in the Energy Sector or Water and Wastewater Systems Sector – has the potential to cascade and create significant impacts to other regions. Currently, the ESS has dependencies on the sectors of Communications and Information Technology and interdependencies with the sectors of Energy, Transportation Systems, Water and Wastewater, Government Facilities, and Healthcare and Public Health (DHS 2014, 2015a). Descriptions of select dependencies and interdependencies are provided below.

Communications: Provide essential services to ESS for daily operations and other activities. Of particular importance is ESS response coordination communications and public alert and warning.

Energy: Fuel and electric power are essential for operations within the ESS. This includes ESS response activities and daily business operations, movement of resources, and response coordination.

Information Technology: Provides essential services to the ESS in support of a variety of cyber-related assets and essential to operations and fulfillment of mission responsibilities. With increasing dependency on cyber-related assets and systems, disruptions or degradation of service would significantly impact the ESS, including the capability to adequately protect the public and safely and quickly respond to emergencies.

Transportation Systems: Secure and effective movement of personnel, resources, and services over multiple modes is required for the ESS. Specifically, response vehicles must be able to transport people, resources, and services to and from incident areas.

Water and Wastewater Systems: Critical for sustaining communities and infrastructure before, during, and after emergencies and is a basic human need vital to human health. For example, the ESS relies on water in response to fires and natural disasters (e.g., bottle water distribution) (DHS 2014, p. 20; 2015a, p. 4, 9–10).

In addition to external dependencies and interdependencies between sectors, the ESS also experiences internal interdependencies similar to other sectors. This is because each responder discipline within the ESS is interdependent on one another for continued functioning. For example, law enforcement secures emergency scenes for fire services and EMS to provide needed services. Additionally, public works ensures roadways are clear of debris to facilitate emergency scene access for other response disciplines. Today, the continual operation of the ESS is dependent and interdependent on other infrastructure sectors. Greater dependences and interdependencies, especially in the cyber realm related to communications and information technology, create the potential that even a localized disruption will have the ability to cascade to other sectors. This is in addition to vulnerabilities within the global and national supply chains that can pose significant disruptions to public safety and security.

Sector Vision, Goals, and Priorities

In alignment with the NIPP, each SSA develops a specific vision and/or mission for their respective infrastructure sector, which is defined in individual SSPs. Listed below are the specific vision and vision statements for the ESS.

Vision Statement: 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.

Mission Statement: Save lives, protect property and the environment, assist communities impacted by disasters, and aid recovery during emergencies (DHS 2015a, p. 26).

In addition to defining the vision and/or mission, the ES SSP identifies specific goals and priorities aligned with the five overall national goals defined in the NIPP, which are provided below.

Sector Goals

1. Continuous growth and improvement of sector partnerships to address risk mitigation and resilience efforts (*NIPP Goal #4*).
2. Support an information sharing environment for information, intelligence, and incident reporting (*NIPP Goals #4 and #5*).
3. Employ a risk-based approach to improve the preparedness and resilience (*NIPP Goal #1*).
4. Improve operational sustainability, resilience, and recovery capacities following an incident (*NIPP Goals #2 and #3*) (DHS 2015a, p. 27).

Sector Priorities

1. Utilize collaborative approaches to strengthen critical infrastructure protective planning and decision-making.
2. Develop and promote information sharing via councils and new, innovative processes and technologies to support protective programs; share risk, capacity building, and model practices information; and improve resource sharing systems and standards.
3. Identify and implement an approach/process to assess and prioritize risk and capability gaps in the ESS to enhance the resilience and recovery capabilities following an incident.
4. Develop and report metrics to measure effectiveness of efforts and gather a means to measure effectiveness (DHS 2015a, p. 27).

Conclusion

The ESS encompasses critical missions that if significantly disrupted or degraded would result in disastrous consequences to the safety and security of US citizens, protection of critical infrastructure, and overall public safety and security. For example, successful intentional cyber or physical attacks on ESS assets could impact domestic emergency response and the provision services to individuals in need. This is in addition to the ever-present risks from natural hazards, which is increasing due to climate change. Therefore, the risk profile of the ESS continues to evolve. These risks include actions happening on the world stage as well as actions within numerous dependent and interdependent infrastructure sectors. Per the NIPP, risks must be continuously evaluated and addressed, especially in the ESS due to its role in US domestic security.

Cross-References

- ▶ Critical Infrastructure Protection
- ▶ Critical Infrastructure: Communications Sector
- ▶ Critical Infrastructure: Energy Sector
- ▶ Critical Infrastructure: Government Facilities Sector
- ▶ Critical Infrastructure: Healthcare and Public Health Sector
- ▶ Critical Infrastructure: Information Technology Sector
- ▶ Critical Infrastructure: Transportations Systems Sector
- ▶ Critical Infrastructure: Water and Wastewater Systems Sector
- ▶ Department of Homeland Security

References

Green, J. (2016, February 26). DHS: Hackers increasingly targeting emergency systems. WTOP. Retrieved from https://wtop.com/j-j-green-national/2016/02/dhs-hackers-increasingly-targeting-emergency-systems/

McGinnis, K. (2004). *Rural and frontier emergency medical services: Agenda for the future*. Kansas City: U.S. National Rural Health Association.

Miller, R. (2006). Hurricane Katrina: Communications and infrastructure impacts. In B. Tussing (Ed.), *Threats at our homeland: Homeland defense and homeland security in the new century – A compilation of the proceedings of the first annual homeland defense and homeland security conference* (pp. 191–204). Carlisle Barracks: U.S. Army War College.

National Center for Frontier Communities. (*2013). Population densities of frontier areas in the United States*. Retrieved from http://frontierus.org/wp-content/uploads/2014/09/2010_frontier-areas-and-pop-densities.xlsx

National Infrastructure Advisory Council. (2007). *The prioritization of critical infrastructure for a pandemic outbreak in the United States: Final report and recommendations*. Washington, DC: U.S. Department of Homeland Security, National Infrastructure Advisory Council.

National Institute of Justice. (2004). *Research for practice: Law enforcement technology – Are small and rural agencies equipped and trained*. Washington, DC: U.S. Department of Justice, Office of Justice Programs, National Institute of Justice.

Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina. (2006). *A failure of initiative: Final report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina* (Report 109–377). Washington, DC: U.S. Government Printing Office.

Simpkins, B. (2015). *2014–2015 national rural training needs assessment – volume II: Assessing capability and training needs within rural communities*. Richmond: Eastern Kentucky University, Justice and Safety Center.

U.S. Department of Defense. (2011). *Strategy for operating in cyberspace*. Washington, DC: U.S. Department of Defense.

U.S. Department of Homeland Security. (2012). *Emergency services sector cyber risk assessment*. Washington, DC: U.S. Department of Homeland Security.

U.S. Department of Homeland Security. (2014). *Sector risk snapshots*. Washington, DC: U.S. Department of Homeland Security.

U.S. Department of Homeland Security. (2015a). *Emergency services sector-specific plan: An annex to the NIPP 2013*. Washington, DC: U.S. Department of Homeland Security.

U.S. Department of Homeland Security. (2015b). *Intelligence assessment: Cyber targeting of the U.S. emergency services sector limited, but persistent*. Washington, DC: U.S. Department of Homeland Security, Office of Intelligence Analysis.

U.S. Department of Homeland Security. (2015c). *National preparedness goal* (2nd ed.). Washington, DC: U.S. Department of Homeland Security.

U.S. Fire Administration. (2007). *Mitigation of the rural fire problem: Strategies based on original research and adaptation of existing best practices*. Emmitsburg: U.S. Department of Homeland Security, Federal Emergency Management Agency, U.S. Fire Administration.

U.S. Government Accountability Office. (2008). *Critical infrastructure protection: Further efforts needed to integrate planning for and response to disruptions on converged voice and data networks (GAO-08-607)*. Washington, DC: U.S. Government Accountability Office.

U.S. Government Accountability Office. (2014). *Critical infrastructure protection: More comprehensive planning would enhance the cybersecurity of public safety entities' emerging technology (GAO-14-125)*. Washington, DC: U.S. Government Accountability Office.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act (Public Law 107-56). 2001, October 26.

Winton, R., & Queally, J. (2016, January 15). FBI is now convinced that couple tried to detonate bomb in San Bernardino terror attack. *The Los Angeles Times*. Retrieved from http://www.latimes.com/local/lanow/la-me-ln-fbi-san-bernardino-bombs-20160115-story.html

Further Reading

Baggett, R., & Simpkins, B. (2018). *Homeland security and critical infrastructure protection* (2nd ed.). Santa Barbra: Praeger Security International.

Lewis, T. (2014). *Critical infrastructure protection in homeland security: Defending a networked nation* (2nd ed.). Hoboken: Wiley.

U.S. Department of Homeland Security. (2013). *NIPP 2013: Partnering for critical infrastructure security and resilience*. Washington, DC: U.S. Department of Homeland Security.