CISA
CYBER+INFRASTRUCTURE

Emergency Services Sector Landscape

AUGUST 2019

U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency

Contents

Executive Summary

The Emergency Services Sector (ESS) comprises an estimated 4.6 million career and volunteer professionals within five primary disciplines: Law Enforcement, Fire and Rescue Services, Emergency Medical Services, Emergency Management, and Public Works. Encompassing a wide range of emergency response functions, the ESS saves lives, protects property and the environment, assists communities impacted by disasters, and aids recovery from emergencies. ESS operations and functions support each of the other 15 critical infrastructure sectors and assist in maintaining public safety, security, and confidence in the government.

Multiple factors may affect the critical infrastructure security and resilience posture of the ESS. These factors, which influence the current operating environment and associated decision-making processes, stem from environmental, technological, human, and physical causes. 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, or long-term economic loss.

The following are five major focus areas for Emergency Services Sector security and resilience risk management planning consideration.

Operational Hazards: Serving and protecting the public routinely exposes emergency services (ES) personnel to the adverse conditions (for example, threats of violence or hazardous materials) affecting the communities they serve. This role requires ES personnel to maintain a high level of threat awareness and associated response capabilities, as well as the capacity to respond to an increasing number of complex challenges. ES personnel perpetually face the challenge of sustaining response levels to existing threats, together with responding to evolving threats requiring new or expanded sector capabilities.

Cybersecurity: The ESS is subject to a wide range of risks stemming from cyber threats and hazards. Sophisticated cyber threat actors and nation-states exploit opportunities to steal information and disrupt or threaten the delivery of essential services. The influx of new mobile technologies that enhance ES organizations' capabilities have altered the vulnerability and threat landscape affecting the sector.

Natural Hazards: Natural hazards—adverse events caused by Earth's natural processes, such as floods, tropical cyclones, wildfires, tornadoes, earthquakes, and tsunamis—have the potential to cause substantial loss of life and property damage. Responding to disasters caused by natural hazards is one of the ESS's primary functions, and the sector maintains robust response capabilities for all types of emergencies. However, the increasing incidence and severity of natural hazards can exacerbate existing challenges to effective response.

Criminal Activities and Terrorism: Criminal activities and terrorism—the use of violence and intimidation in the pursuit of personal or political aims—can affect the ESS's ability to prepare for and manage emergencies, enforce the law, and provide public safety. Security and resilience issues that hinder the ability of ES personnel to provide essential services include attacks on personnel and assets, theft of vehicles and equipment, and malicious use of unmanned aircraft systems.

Crosscutting Issues: Issues stemming from infrastructure, social, technology, and economic changes have the potential to disrupt ES, overburden ES organizations, and increase capital expenditures. For the ESS, crosscutting security and resilience issues include managing access and re-entry challenges near an incident or event, aging infrastructure, changing populations, and interdependencies with other sectors.

This document provides a sector-specific characterization of relevant factors and decision-making drivers influencing the current operating environment and security and resilience posture of the ESS. Government and sector partners may use this document to help identify and address factors that could have adverse effects on the security or resilience of facilities, personnel, and operations. This document does not represent a compendium of vulnerabilities, nor is it a sector risk assessment. The different factors discussed in this document have been included because they influence the critical infrastructure security and resilience posture of the sector as a whole. Therefore, these factors are discussed from a sector-wide perspective and may not apply to all segments within the sector. As the security and resilience operating environment for the ESS changes, this document may be updated.

Operational Hazards

Emergency Services (ES) 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. In serving and protecting the public, ES personnel may be exposed to a variety of harmful situations, for example, potential exposure to toxic chemicals when responding to a hazardous material spill or physical abuse when attempting to render aid to an injured person. Effects may be acute and immediately felt but may also accumulate over time, potentially degrading physical and mental health. Security and resilience issues relating to operational hazards include the threat of exposure to hazardous materials, operational burnout associated with elevated and prolonged stress, and the potential to encounter violence and assaults while performing duties.

Exposure to Hazardous Materials

When responding to incidents, ES personnel may face the same hazards affecting the individuals they are attempting to assist. The presence of chemical, biological, radiological, nuclear, or explosive (CBRNE) substances, incomplete or inaccurate cargo information, or exposure to other unknown substances can create a dangerous response environment for ES personnel.

- **CBRNE:** CBRNE substances represent a broad range of potential threats that may be present at an incident, and identifying the type and properties of these substances requires training. Exposure can have serious long-term consequences. Among emergency medical services (EMS) workers, exposure to harmful substances such as potentially infectious fluids (e.g., bodily fluids) was the second leading cause of occupational injuries after body motion injuries.[1] Similarly, exposure to powerful synthetic opioids such as fentanyl and carfentanil, especially when encountering illicit production or milling operations, endangers the safety of responders and requires new approaches to maintain safety.
- **Incomplete/Inaccurate Cargo Information:** ES personnel rely on cargo information to help inform their response, and inaccuracies or incomplete information can lead to unnecessary exposures. Personnel must rely on sensors on either their persons or their vehicles to identify the presence of unexpected dangerous substances.
- **Unknown Substances:** ES personnel can be exposed to unknown substances intended for others, for example, when screening packages for hazardous materials. Similarly, ES personnel may respond to an incident and discover onsite, or after the fact, that hazardous materials were present.

Operational Burnout

ES personnel have demanding roles and responsibilities. In many cases, the daily duties of ES personnel require interacting with and providing aid to people on their worst day. The stress of providing emergency response coupled with high operational tempos, workplace constraints, training and certification requirements, and the pressures of daily life can lead to operational burnout. Both personnel and communities may suffer from the results of operational burnout. Public expectations have increased despite limited funding and resources. These constraints encumber ES organizations' ability to retain experienced personnel and recruit new personnel, which can contribute to an overall reduction in available essential services.

- **Operational Tempo:** ES personnel often work extended shifts of 10 hours or more. A recent study of a sample of EMS personnel found that the risk of injury and illness increased with shift length.[2] A similar study of firefighters found additional 24-hour shifts—beyond a standard work schedule of between eight and eleven 24-hour shifts per month—and increased job demands were associated with elevated blood pressure.[3] Heart attacks and strokes caused the majority of on-duty deaths in 2017.[4] In addition, extended periods of heightened awareness in anticipation of emergencies

happening throughout a shift may cause high levels of stress. ES personnel are frequently less likely to ask for help than those in other professions, allowing stressors to go undetected and unaddressed.[5]

- **Increased Public Expectations:** The public increasingly expects first responders to possess the capabilities to respond to emergencies of all kinds. For example, firefighting has become a smaller portion of the specialized services fire departments provide to their local communities, giving way to calls for EMS or other specialized services. Trying to meet the expanded demand stresses ES organizational budgets, increases personnel training requirements, and raises costs associated with equipment maintenance.
- **Funding and Resource Constraints:** Diminished government budgets may affect the capacity of the ESS to adequately address, anticipate, or prepare for changes in the sector's risk profile. As costs increase for healthcare, personnel, fuel, and equipment maintenance, along with the demand for essential services, ES organizations may find it difficult to rapidly respond to incidents, maintain the required capabilities, train specialized teams, or replace aging equipment necessary to support their communities.
- **Workforce Shortages:** Workforce shortages in any of the ESS disciplines may hinder their ability to respond effectively and efficiently. When ES organizations are challenged to perform a greater amount of work with fewer personnel, this situation can cause more rapid burnout as well as increased spending (e.g., for overtime and equipment maintenance).

Violence and Assaults

Potential violence and assaults against first responders are major security and resilience issues, which can manifest as physical assaults as well as verbal threats and abuse. In performance of their duties, ES personnel routinely interact with unruly individuals. EMS personnel face a growing number of violent incidents (e.g., physical assaults, verbal threats and abuse, and intimidation), which nearly doubled from approximately 1,800 incidents in 2009 to 3,500 in 2016.[6] Law enforcement officers are three times more likely to sustain injury than all other workers, and assault-related injuries to law enforcement officers grew nearly 10% annually between 2003 and 2011 while rates of injuries in all other professions remained unchanged, according to data from the National Institute of Occupational Safety and Health.[7]

- **Physical Assaults and Related Injuries:** While training helps all first responders address such threats, assaults can nonetheless result in serious injury to first responders. The Centers for Disease Control estimates that 3,500 EMS workers sought treatment at an emergency department in 2016 because of violence.[8] Because ES personnel generally receive training to reduce the chance of personal injury during an emergency, some may blame themselves for becoming the victim of an attack, which can negatively affect their mental health. In addition, physical assaults and concerns about the safety of first responders can have negative impacts on retention and recruitment, hurting the organization.
- **Verbal Threats and Abuse:** First responders may face verbal threats and abuse from patients, individuals being detained, or bystanders. Reasons can range from anger over the timeliness of ambulance arrival to frustration borne out of helplessness in the situation. Verbal abuse adds stress to an already stressful situation and over time can contribute to larger health issues for ES personnel.

Case Study: Protecting the Protectors

Numerous studies have found that a significant percentage of first responders to the World Trade Center attacks on 9/11 have had post-traumatic stress disorder (PTSD), as well as associated cognitive difficulties and major depression (for example, PTSD is reported as anywhere from 7% to 24%, depending on the first responders studied and the number of years since the event). Medical team workers responding to the 2011 Tōhoku, Japan earthquake and tsunami are reported to have suffered from clinical depression at a rate of over 20%. Two police officers who responded to the Pulse nightclub shooting in Orlando, Florida, have spoken publicly about the resulting PTSD; one, deemed disabled, was ultimately relieved of his duties.

Struggling in the wake of significant—perhaps historical—tragedies is perhaps unsurprising, but first responders face challenging situations as a matter of course. Their duties lead them into high-stress—and often high-risk—scenarios, often in close succession. Stressors include repeated exposure to death, grief, and injury, as well as threats to personal safety. With limited time to process these experiences, our front line may experience PTSD, depression, suicidal ideation, and a host of related conditions. Worse still, many of those who serve may refuse to seek help for various reasons: some feel they should be able to handle the stress on their own, some recognize a stigma attached to behavioral health conditions, and some lack the necessary time and financial resources.

Fortunately, a cultural shift has taken place, emphasizing awareness and support programs to combat these occupational hazards. ES leaders have implemented steps to safeguard the physical and mental health of their personnel. New staff should be carefully screened for suitability to handle extreme stress, and all staff may benefit from mental health training. Providing planning, training, and clear roles and reporting structures in advance of an event provides comfort through a sense of preparedness. During an event, leaders should continually assess the team's welfare, and team members can employ a "buddy system" for both stress checks and physical safety. Follow-up procedures for particularly difficult experiences should include counseling and debriefing for responders, as well as time away from stressful assignments, when possible.

Cybersecurity

The ESS is subject to a wide range of issues stemming from cyber threats and hazards. Sophisticated cyber actors and nation-states exploit opportunities to steal information and disrupt or threaten the delivery of essential services. The influx of new mobile technologies that enhance ES organizations' capabilities may also alter the vulnerability and threat landscape affecting the sector.

Issues of higher cybersecurity risk for the ESS include advanced persistent threat (APT) attacks, distributed denial of service (DDoS) attacks, increased connectivity and disruptive digital technology, and malware and ransomware. Recognizing and mitigating these issues could help to limit cyber intrusions.

Advanced Persistent Threat

Coordinated campaigns by motivated cyber threat actors pose significant risk, and opportunities will likely continue to be found in for attacks on cyber assets. APTs can exploit these opportunities to establish persistence in a network and acquire sufficient access to achieve objectives (e.g., exfiltration of sensitive information), given enough time and resources. An ES organization's information systems could be compromised by an APT, hindering response efforts. VPNFilter and Dragonfly represent recent prominent examples of malware and a cyber threat actor that could affect the sector.

- **VPNFilter:** In May 2018, Cicso's Talos Intelligence Group announced its research into a modular malware system they named VPNFilter, which had infected more than 500,000 devices. The malware uses vulnerabilities in a range of network devices—primarily internet routers—to install a persistent foothold in the targeted devices, which can be used to deploy further modular malware on the devices.[9]
- **Dragonfly:** Russian government cyber threat actors have been targeting U.S. critical infrastructure sectors since at least March 2016 in a coordinated campaign of malware attacks collectively named Dragonfly. The threat actors used a combination of spear phishing (highly targeted emails with malicious attachments) and watering hole attacks (introducing malware through well-known industry trade publications' websites) to collect user credentials. The threat actors were able to establish footholds in the target networks and conduct network reconnaissance, move laterally, and collect sensitive or proprietary information.

Distributed Denial of Service Attacks

DDoS attacks are a growing threat, generating immense bandwidth loads to the point of disruption or creating openings for malware to be deployed. As ES organizations introduce more Internet-connected devices (see Increased Connectivity and Disruptive Digital Technology below) into their operations, more vulnerabilities to DDoS will arise. Devices used in response activities that are connected to the Internet could have their functionality diminished by DDoS, rendering response activities less effective. Botnets have been used to leverage Internet-connected devices to carry out DDoS attacks, and techniques such as amplification potentially extend the potential for disruption. The sector's reliance on telephony, especially for public services answering points (PSAPs), potentially exposes ES organizations to telephonic denial of service attacks.

- **Botnets:** Botnets are collections of Internet-connected devices that have been infected with malware to respond to specific requests from a command and control entity. Potential devices range from home computers to Internet of Things (IoT) devices. Botnets can be used to generate massive amounts of Internet traffic to a specific target with the intention of disrupting essential services. A recent high-profile example was the Mirai botnet, which was used in October 2016 in a DDoS attack

on a major domain name system (DNS) service provider. The attack flooded 1.2 Terabits per second (Tbps) of Internet traffic (at the time, the highest volume of DDoS traffic ever recorded) managed by the DNS provider and shut down many well-known websites. At the height of the attack, millions of users were denied Internet services in North America and Europe. Similar to the previous September 2016 Mirai attack, the DNS attack employed millions of compromised Internet-connected security cameras to simultaneously conduct the attack.[10]

- **Amplification:** Amplification refers to a technique in which a cyber threat actor abuses Internet-connected devices such that they respond to a small packet of code from the attacker by sending large packets of data to a target as part of a DDoS attack. The effect amplifies the bandwidth sent by the threat actor, resulting in much larger amounts of data flooding the target. Unlike with botnets, the threat actor does not necessarily need control of the device. Instead, a threat actor abuses the devices' intended functionality to respond to requests and causes the responses to flood a target's servers. Memcached DDoS attacks, a specific type of amplification attack, resulted in 1.3 Tbps and 1.7 Tbps of Internet traffic in separate attacks in March 2018, though no critical services were disrupted.[11]
- **Telephonic Denial of Service (TDoS):** Cyber threat actors can leverage malicious code to flood public services answering points with fraudulent calls and disrupt operations. Malicious code can abuse mobile phones' functionality not only to place fraudulent calls to 911 without the users' knowledge or consent, but also to propagate the malicious code to other users and create more calls.[12]

Increased Connectivity and Disruptive Digital Technology

Computer-aided dispatch (CAD) improves the capabilities of operators. Location services, fleet management, environmental sensors on responders, and other digital technology improvements aid responders with increased connectivity. This increased connectivity coupled with disruptive digital technology—new technology that displaces an established technology or means of operation—may also create new risks if the systems are not properly secured. In general, combining physical and digital technologies may introduce new risks, including increased points of access through which malicious code could be introduced or data could be stolen, and the potential for cascading failures due to interconnectivity.

- **Wearables:** With the forthcoming Nationwide Public Safety Broadband Network, ES personnel could expand use of wearable communications devices and sensors that can provide beneficial functions such as authentication, heart rate monitoring, video recording, hands-free communication, or location tracking. These new and expanded capabilities represent greater security needs for data and communications.
- **Next Generation 911:** Next Generation 911 systems operate using digital (rather than analog) technologies. The use of modern digital networking offers many benefits that enhance PSAP capabilities, but it also requires administrators to manage associated cyber threats and vulnerabilities.
- **Increased Points of Access:** An expanding footprint of networked devices introduces more points of potential targets for cyberattack in the network. Both physical (e.g., locations for input or display devices) and cyber (e.g., network ports) points of access could be exploited.
- **Cloud Services:** ES organizations are increasingly incorporating cloud services into their operations. Cloud software-as-a-service (SaaS) is leveraged to enhance response capabilities. Although cloud services offer benefits, such as high availability, advanced data analysis and storage, and decreased ownership cost, new cybersecurity concerns are associated with those benefits. Cloud services share many of the same cybersecurity issues as physical, onsite information technology (IT) (e.g., denial of service, APT, stolen credentials, and phishing) yet also exhibit virtual susceptibility to attacks, including malicious control of virtual machines and attacks on systems running virtual processes.

- **Cascading Failures:** Automated systems that are dependent on interconnected devices may be subject to cascading failures that result from disruptions along the network of devices. A disruption within a chain of interconnected devices can have drastic cascading effects on the safety of ES personnel or the availability of supporting capabilities of ES personnel.

Malware and Ransomware

Malware, including ransomware, is commonly used in attacks on many types of ES organizations' networks. Malware could be used to steal an organization's information, to steal data such as personally identifiable information or medical information, or to interrupt business operations. CryptoWall, Emotet, and WannaCry are three prominent recent examples that have affected several critical infrastructure sectors.

- **CryptoWall:** CryptoWall is among the most commonly used ransomware varieties, with various forms of the ransomware targeting hundreds of thousands of individuals and businesses. The ransomware arrives on the affected computer through spam emails. Not only does it encrypt files and prompt the business to pay for the key, it hides inside the operating system and adds itself to the Startup folder, accesses passwords, and deletes volume shadow copies of files so that data restoration is difficult or impossible. Some reports estimate that CryptoWall has grossed over $325 million in ransom payments since 2014.[13]
- **Emotet:** Predominantly targeting the financial sector but affecting municipalities as well, Emotet represents an especially complex type of malware because it is advanced, modular, and polymorphic (i.e., it changes its own content to evade signature detection). Potential consequences include temporary or permanent loss of sensitive or proprietary information, disruption to regular operations, financial losses incurred to restore systems and files, and potential harm to an organization's reputation.
- **WannaCry:** In May 2017, WannaCry ransomware infected organizations all over the world, encrypting and paralyzing the systems. WannaCry exploited security vulnerabilities in Windows computer systems. Information about the Windows code flaw was released in leaked National Security Agency documents, and although a patch was developed to eliminate the security vulnerability, many organizations did not download the upgrade before the attack. The ransomware affected mostly business control systems, although the malware mechanism used could be adapted to disrupt process control systems.

Supply Chain Cybersecurity

ESS assets and networks are susceptible to compromised vendor communications associated with the sector's supply chain. Email phishing attempts from presumed trusted vendor email accounts are becoming more frequent. Successful phishing attempts could allow cyber threat actors remote access to enterprise networks and the opportunity to escalate attacks to operations infrastructure. Trusted contractors and vendors may have legitimate remote access to provide services; however, this access could turn problematic if the contractor or vendor has been compromised. The supply chain for software itself represents another cybersecurity issue, as compromised software introduced along the supply chain could be used to attack ESS networks.

- **Third-Party Attacks:** Cyber threat actors have targeted critical infrastructure subcontractors' networks to abuse access the subcontractor might have to the target organization. This abuse of trust in software suppliers and subcontractors can affect even well-protected organizations.
- **Software Supply Chain:** In 2017, software supply chain attacks increased dramatically across all sectors.[14] In attacking software providers, cyber threat actors replace legitimate business software with maliciously modified versions, unbeknownst to end users. If an ESS organization attempts to

download, for example, the latest version of previously trusted software, it receives the malicious version instead.

Case Study: Thwarting TDoS Attacks

In October 2016, an 18-year-old hacker played a digital "prank" that ultimately targeted multiple 911 departments in Arizona, California, and Texas. He tweeted a link to a webpage that, when visited on a mobile phone, would cause the phone to place repeated 911 calls. The resulting volume of calls to 911 operators threatened availability of services. Such a strategy is perhaps clever but not overly complicated to enact, yet it is difficult to foresee and prevent. As people place more emergency calls from cell phones, the potential for TDoS attacks to resemble DDoS attacks rises.

Recent years have seen an exponential increase in the frequency and intensity of DDoS events. In response to this escalating threat, the U.S. Department of Homeland Security (DHS) is working on a multimillion-dollar effort to protect critical digital systems from DDoS attacks. DHS has provided $14 million in grants for DDoS prevention studies, including preventing TDoS attacks. Results to date include a prototype technology that can detect and thwart fake telephone calls and selection of multiple partners to pilot the technology. However, there are concerns about blocking any calls, even likely false ones, to 911 centers, so the technology must be made infallible or another solution must be sought.

Natural Hazards

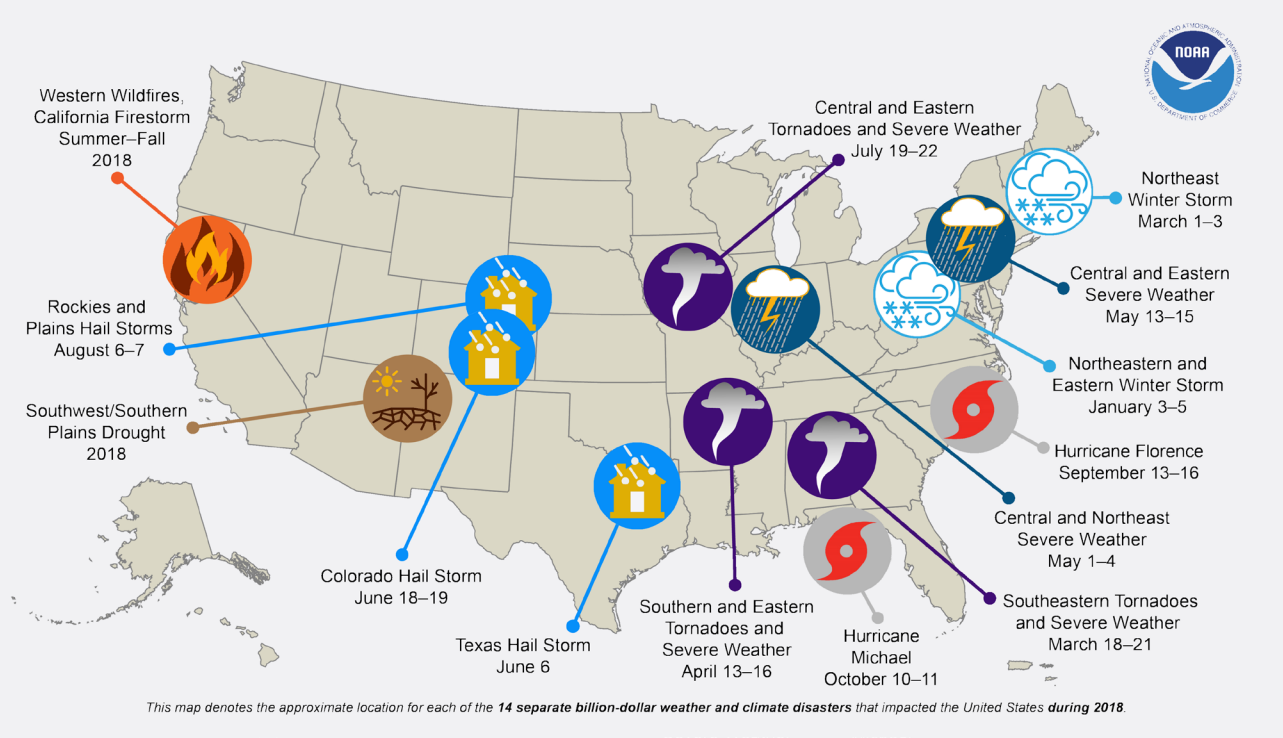
Natural hazards include major adverse events caused by Earth's natural processes, including floods, cyclones, wildfires, tornadoes, earthquakes, and tsunamis. Natural hazards can cause disasters that result in loss of life and property damage as well as economic damage and disruption or destruction of facilities and operations. The severity of a disaster is measured in terms of lives lost, economic disruption, and the affected population's ability to rebuild.

Responding to disasters caused by natural hazards is one of the ESS's primary functions, and the sector maintains robust preparedness and response capabilities for all types of natural hazards. Major issues of natural hazards for the sector include larger and more severe natural hazards and the environmental dangers that arise because of natural hazards.

Cost, Frequency, and Severity of Natural Disasters

Recent billion-dollar-loss natural disaster events in the United States include Atlantic and Gulf Coast hurricanes, northeastern winter storms, freezing in southeastern states, tornadoes and hail storms in central states, and wildfire and drought in western states. In 2018, the United States experienced 14 billion-dollar disasters, with total damage costs across all sectors exceeding $91 billion. The total number of these disasters is the fourth-highest behind 2011, 2017, and 2018.[15] Figure 1 provides a map of these events. Such large-scale events have cascading impacts across sectors and regions. More extreme weather increases the geographic magnitude and severity of events caused by natural hazards, requiring a surge of ES resources, often for extended periods, while also straining resources in partnering regions that might otherwise supply mutual aid. Such events cause an increased hazard to responders while often disrupting critical services needed for effective response.

Figure 1. *2018 U.S. Billion-Dollar-Loss Natural Disaster Events*
Source: National Oceanic and Atmospheric Administration (NOAA)



- **Emergency Management:** Disaster impacts are increasing; large-scale disasters such as Hurricane Harvey can make management difficult from the outset. Wide-ranging damage can affect primary and secondary locations for emergency operations centers, requiring makeshift workarounds and delaying response efforts. High winds, wildfires, ice storms, and other hazards often damage communications infrastructure, compounding challenges with managing increased communications needs (see Crosscutting chapter below).
- **Public Works:** Major natural hazards typically will cut off or drastically restrict access to affected areas. This hinders response efforts and may initially curtail debris removal operations, damage assessments, and restoration efforts.
- **Police, Fire, and EMS:** Severe natural hazard events can have impacts on primary operating and support facilities (e.g., local police stations, fire houses, and storage facilities) and stress organizational preparedness efforts. Primary facilities may be damaged by fire or flooding or may experience a prolonged power disruption, reducing response capabilities. Prolonged emergencies or preexisting conditions caused by extreme weather patterns (e.g., droughts, floods, and wildfires) may complicate response efforts, strain limited resources, or increase operational burnout.

Environmental Dangers

ES personnel may be exposed to health risks associated with natural disasters, including toxins dispersed from flooding (e.g., sewer and wastewater), carcinogens as by-products of fires, or infectious diseases. Also of concern during ESS operations are physical hazards caused by natural disasters, such as falling or flowing debris, building or roadway instability, or extreme heat or cold.

- **Release of Toxins:** Flooding can cause release and dispersion of unknown toxins, which creates a health hazard for ES personnel. Floodwaters can contain human and livestock waste; household, medical, and industrial hazardous waste; coal ash (which contains arsenic, chromium, and mercury); or other contaminants that cause adverse health effects.
- **Carcinogens as By-Products of Fires:** Exposure to wildland smoke, even at low-to-moderate levels, represents a safety and health hazard to wildland fire personnel. Wildland fire smoke contains a variety of inhalation irritants including carbon monoxide, aldehydes, particulate matter, crystalline silica, and polycyclic aromatic hydrocarbons. Some of the compounds in wildland fire smoke are confirmed carcinogens or suspected carcinogens.[16]
- **Infectious Diseases:** Pandemics—a type of natural hazard themselves—affect ES organizations as some ES personnel, or members of their families, will likely fall ill during a pandemic, reducing workforce availability just as demand for emergency services increases. Conditions in the wake of hurricanes and other natural hazards can increase the probability of the spread of infectious diseases.
- **Physical Hazards:** While public works personnel will clear, remove, and dispose of debris from natural hazards, ES personnel operating in time-sensitive situations need to take extra precautions to avoid physical hazards, which can impede their operations.

Case Study: Responding to Flooding and Fires at a Chemical Plant

Hurricane Harvey led to explosions at a major U.S. chemical facility in Texas. The U.S. Chemical Safety Board (CSB) investigated the event and found that the facility had established—and did follow—policies and safeguards for hurricanes. These included elevating portable equipment to keep it out of floodwater, staging sandbags, acquiring a boat and forklift that could operate in floodwater, and activating a "ride-out crew" who would remain onsite during the storm. Workers also moved organic peroxides from low-temperature warehouses, where the peroxides were normally stored, to nine refrigerated trailers used for shipping. Six of the trailers were relocated to a high-elevation area, but three could not be moved and were in danger of losing refrigeration. When the storm's devastating potential became evident, plant officials determined that the refrigerated trailers might very well lose power, causing the organic peroxide products inside to combust within a few days. Plant personnel alerted local emergency responders, who evacuated the ride-out crew and then implemented an evacuation zone around the site.

Concurrent emergency response remained underway throughout the region to address the havoc in Harvey's wake. To facilitate transport of rescue resources through the area, local officials kept the main highway open, although it ran through the evacuation zone. Five police officers drove on this route through a cloud of smoke, later confirmed as coming from the chemical manufacturing facility, and shortly thereafter began to have nausea, headaches, sore throats, and watering eyes. Officials then shut down the highway, but a total of 21 people sought medical attention from reported exposure to the noxious fumes. Within 24 hours of the road closure, the chemicals in all three at-risk trailers caught fire.

The status of the chemicals in the six remaining trailers was unclear. On September 3, eight days after Harvey made landfall in Texas, emergency responders entered the site and conducted a controlled burn of the remaining trailers to end the evacuation and allow citizens to return to their homes.

Criminal Activities and Terrorism

Criminal activities and terrorism affecting critical infrastructure make headlines around the world almost every day. Terrorism, which can be described as the use of violence and intimidation in the pursuit of ideological aims, can take many forms, including chemical, biological, radiological, nuclear, and explosive attacks.

In the ESS, security and resilience issues regarding criminal activities and terrorism include direct and secondary attacks as part of violent extremism, theft of vehicles and equipment, and malicious use of unmanned aircraft systems (UASs). Recognizing and mitigating these risks could help to limit the financial, operational, and human impacts of criminal activities and terrorism.

Homicides, Assaults, and Targeted Attacks

Every year, a substantial number of ES personnel are killed or injured in the line of duty. Among all occupations, not just the ESS, police and sheriff's patrol officers count among the highest numbers of workplace homicides. Similarly, ES personnel, not just law enforcement, face some of the highest rates of workplace violence in the course of performing their duties. In addition, terrorists and violent extremists have attacked ES personnel, especially law enforcement, in recent years, and terrorist organizations continue to encourage supporters to carry out both direct and secondary attacks on first responders.

- **Felonious Homicides and Assaults:** In the past five years (2014–2018), 259 law enforcement officers died in the line of duty as a result of felonious incidents. Of these, 109 were killed as part of investigative or enforcement actions, and 53 were killed in ambush-style attacks.[17] In addition, more than 60,000 officers were assaulted in 2017 alone, with more than 17,000 attacks resulting in injuries.
- **Attacks Related to Terrorism and Violent Extremism:** In 2016 and 2017, 15 attacks targeting law enforcement resulted in 12 fatalities and 22 injuries, according to the University of Maryland's Global Terrorism Database.[18] Of the 15 attacks, 6 were perpetrated by people with expressed anti-government or anti-police sentiments; another 4 perpetrators had unknown motivations but nevertheless targeted police or police headquarters. Most attacks involved armed assault on law enforcement, typically shootings of officers or their cruisers. Several other attacks involved incendiary devices targeted at police headquarters.

Theft and Impersonation

ES equipment can be a target for theft; objects of particular interest include response vehicles, uniforms, firearms, access control items (e.g., badges or keys), supplies (e.g., medicine or narcotics), and technological equipment. When an unauthorized person gains access to emergency response vehicles or equipment, the acquisition could lead to a dangerous situation. The theft of emergency response vehicles and equipment may be an indicator of pre-operational activity by a malicious actor or actors that constitutes a potential threat to public safety, as stolen emergency vehicles and equipment have been used to exploit site vulnerabilities, destroy critical infrastructure, and harm people and property.

- **Stolen Vehicles and Equipment:** In the course of responding to an emergency, ES personnel may inadvertently present an opportunity to steal an emergency response vehicle. Focused on the immediate needs of injured people, ES personnel may not fully secure a vehicle when arriving at a scene. Theft of ES equipment not only affects the safety of emergency responders but also jeopardizes their ability to provide timely and effective public safety services.

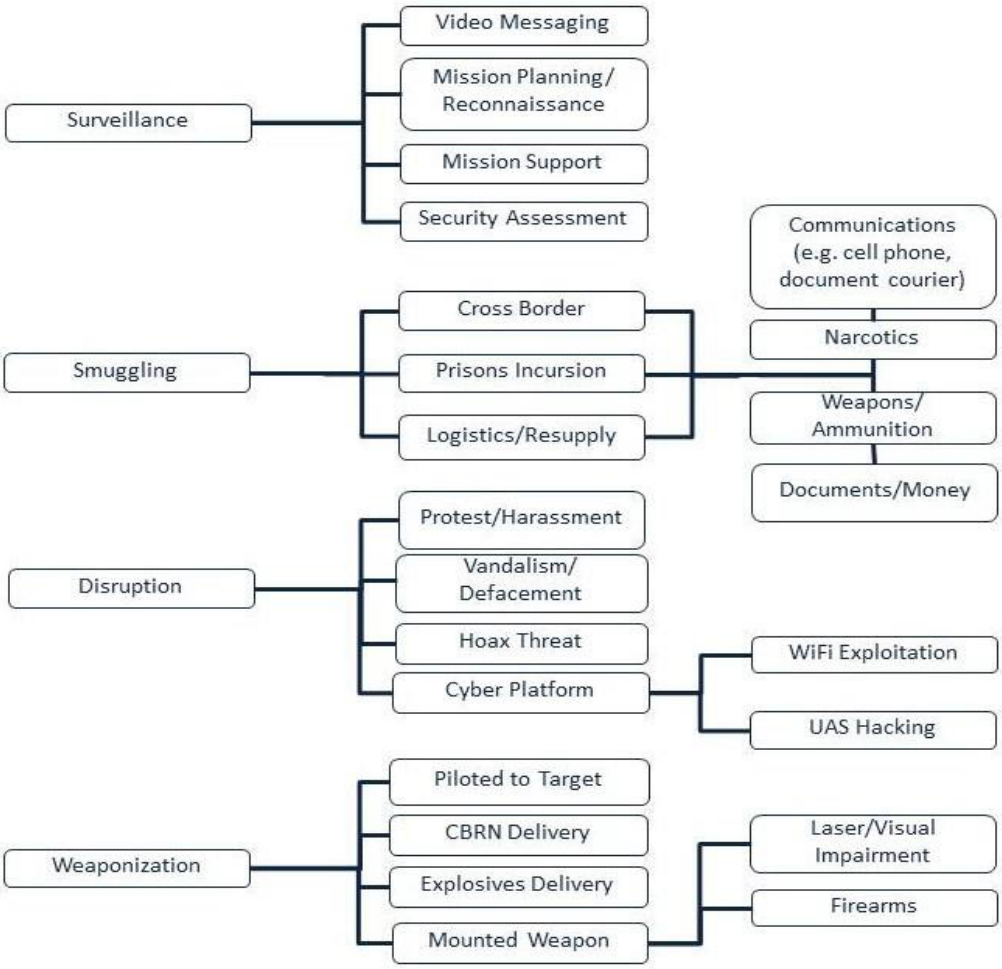
- **Impersonation:** Both international and domestic malicious actors may exploit the public trust in first responders by impersonating first responders to inflict harm, exploit site vulnerabilities, or destroy critical infrastructure. Malicious actions include the acquisition of authentic or fraudulent uniforms, equipment, vehicles, and other items that may be associated with law enforcement, fire, and EMS personnel.

Unmanned Aircraft Systems

UASs offer both promise and peril. They have been used to survey areas affected by natural disasters, such as the city of Houston following Hurricane Harvey, to effect a more informed response.[19] While official use can improve response efforts, non-official use is on the rise, as UASs are commercially available and easy for the layman to use. The upward trend suggests negative encounters with UASs, too, will continue to increase in the near future. UASs could be used for illicit surveillance to target or monitor ES personnel or response operations, to disrupt operations (e.g., interfering with emergency operations or initiating cyberattacks that compromise ES communications and networks), or to cause physical damage (see Figure 2).[20]

- **Surveillance:** UAS video capabilities can be used by adversaries for preoperational planning to monitor and assess security operations at sensitive sites, large-scale events, and law enforcement or emergency response operations.
- **Disruption:** Intentionally or unintentionally, UASs may endanger law enforcement, medevac, firefighter, and other ES flight operations by operating in the same airspace. Adversaries can also direct UASs close to a facility to access, monitor, or attack computer networks and/or monitor or interfere with radio frequency communications. Such UAS proximity to a facility, whether intentional or unintentional, can harass, hinder, or inhibit emergency response operations.
- **Weaponization:** UASs can be central to an attack intended to cause casualties or physical damage; possible strategies include disrupting air traffic, deliberately crashing, and delivering a hazardous payload (e.g., an explosive device or a chemical, biological, or radiological weapon).

Figure 2. *Categories and Examples of Malicious UAS Activity*
Source: DHS I&A



Case Study: Fighting on Two Fronts

From a safe distance, wildfires make for spectacular viewing, as do aerial firefighting teams' efforts to battle the blazes. It is perhaps unsurprising, then, that UAS hobbyists send in their drones to get prime footage. Unfortunately, the response teams find the tiny fliers a nuisance at best, a danger at worst. On at least 22 occasions during the 2018 wildfires, fire aircraft were forced to halt proceedings temporarily when drones were discovered flying close enough to risk collision.

Aerial firefighting requires speed and rapid directional changes, as fliers chase hot spots, swoop downward to release the payload, and quickly fly away. Much of the flying takes place fairly low to the ground, in the same airspace occupied by hobbyist drones. Unauthorized UASs have the potential to distract pilots and crash into planes. Aircraft are somewhat unstable just after release, increasing the risk factor of a UAS encounter. Hobby drones not only threaten the safety of the firefighters—both those in the plane and those beneath them—but also delay the firefighting operations, imperiling citizens and their property.

The increasing frequency of UAS appearances over or near wildfires has occasioned multiple public outreach efforts, including a tagline shared across fire agencies: "If you fly, we can't." Other public tools include the U.S. Department of the Interior's wildfire location data-sharing program, "Current Wildland Fires," and the Federal Aviation Administration's smartphone app, B4UFLY.

Crosscutting Issues

The ESS is subject to several crosscutting issues that stem from infrastructure, social, technology, and economic changes. Crosscutting security and resilience issues include access and re-entry challenges, aging infrastructure, changing populations, communications challenges such as interoperability, and dependencies and interdependencies with other sectors. These issues could disrupt ES operations, overburden ES organizations, and increase capital expenditures.

Access and Re-Entry

Effective control and coordination of access for key response and recovery resources into an affected area before, during, and after an emergency improves the likelihood of successful community recovery. The process of managing access into restricted areas or through emergency zones during an incident is a state or local responsibility and can become increasingly difficult when disasters extend across multiple jurisdictions or involve significant population evacuations.

- **Multi-Jurisdiction:** When an incident extends across jurisdictional boundaries, the number of stakeholders requiring access to conduct damage assessments, protect critical infrastructure, and reestablish essential services increases, adding complexity to response and recovery efforts. A lack of a common approach to access management may hamper restoration efforts, increase recovery costs, and reduce overall operational success.
- **Evacuation:** During incidents that require significant population evacuations, access management is particularly important to ensure coordination of public- and private-sector response and recovery assets, restoration of critical infrastructure and essential public services, and the safe and orderly return of community members back into an affected area. A lack of coordinated access management can cause confusion among stakeholders, negatively affect restoration efforts, and create hardships for both residents and first responders.

Aging Infrastructure

A significant portion of U.S. infrastructure is in need of repair or replacement. The American Society of Civil Engineers 2017 Infrastructure Report Card rated U.S. infrastructure as a whole at D+. Of that, roads received a D; bridges, a C+; ports, a C+; rail, a B; inland waterways, a D; energy, a D+; drinking water, a D; and wastewater, a D+. The state of disrepair and viability of our nation's infrastructure is of great concern to the ESS, as all ES disciplines rely on this infrastructure (e.g., functioning electrical grids, water management systems, roads, and bridges) to perform critical functions. This section highlights issues of concern for these sectors.[21]

- **Roads:** The Nation's roads and highways are commonly overcrowded, in disrepair, and significantly underfunded. In 2014, over $160 billion was wasted in time and fuel owing to traffic delays and congestion. Approximately 20 percent of highways are in poor condition, causing increased costs of vehicle maintenance and repairs. An approximate backlog of over $700 billion in projects awaits funding to repair existing highways, make strategic expansions, and update the highway system (e.g., for safety, operational, and environmental improvements).
- **Bridges:** In the United States, most highway bridges are designed for a life span of approximately 50 years. Of the more than 600,000 bridges in the United States, approximately 40 percent are 50 years old or older, and 9 percent are structurally deficient. Although bridge conditions have improved in recent years, funding for bridges may be inadequate to maintain or improve current capacities. An estimated $123 billion is needed to eliminate the Nation's bridge upgrade backlog.

- **Ports:** The vast majority of the Nation's international trade—99 percent—flows through its ports, accounting for approximately 26 percent of its economy. As the ships carrying this cargo continue to increase in size and capacity, U.S. ports become more congested and less able to accommodate the largest ships. Ports are expected to spend approximately $155 billion from 2016–2020 to expand, modernize, and repair in response to demands of international trade. Connected infrastructure (land, rail, and inland waterway connections to ports) requires commensurate aid, yet funding for these improvements and repairs is lacking.
- **Rail:** The freight rail industry has made important investments and repairs in the past several years to improve its systems and meet future needs. Short rail lines are in need of upgrading and maintenance funding—more so than long-distance lines—to advance in freight car capacity and repair and replace bridges.
- **Inland Waterways:** A total of 50,000 miles of canals, locks, and dams comprise the Unites States' inland waterways system, the majority of which is older than the original 50-year design life of its components. These waterways are an important part of freight transportation, connecting ocean ports with inland transportation hubs and accounting for approximately 14 percent of domestic freight. Age and disrepair with lack of funding result in frequent delays for hours at a time, contributing to economic losses. Although investments have been increasing in recent years, repair and upgrade projects can take decades to complete.
- **Energy:** While energy infrastructure owners—predominantly in the private sector—are investing to ensure long-term capacity and sustainability, the energy sector depends on complex systems composed of assets that vary widely in age and condition. Almost half of U.S. natural gas transmission and gathering pipelines were built in the 1950s and 1960s; annual investments in interstate natural gas pipelines will total more than $2.6 billion through 2030.[22] Aging electricity transmission and distribution lines must be replaced or upgraded; spending on distribution systems grew to $51 billion annually as of 2017, and spending on transmission infrastructure rose to $21 billion annually as of 2016.[23,24]
- **Water and Wastewater:** Renewal and replacement of aging water and wastewater infrastructure has been the top issue for the water industry between 2014 and 2018.[25] Many of the Nation's one million miles of pipes transporting drinking water, which have life spans of 75 to 100 years, were laid in the early to mid-20th century. Replacing pipes, pumps, and other assets will require significant investment. Old wastewater conveyance and treatment systems may not meet the demands of growing populations; an estimated $271 billion in investment will be needed to meet current and future demands.

Changing Populations

Increased population density in urban and suburban areas and changing population characteristics may exacerbate existing risks. Dynamics that could alter the resource requirements for ES organizations include growing populations leading to greater population density, greater mobility, and overall aging of the general population.

- **Population Density:** A growing population may create areas of higher population density, especially in urban centers, which increases response needs. Urban settings also amplify many of the issues surrounding incident management response. The density of the environment and need to facilitate evacuation, secure the scene, and establish restricted areas may stress emergency response resources.
- **Mobility:** Global mobility increases the potential for spread of biological agents and communicable diseases and related loss of able-bodied ES personnel responding to those incidents. Evolving health issues like antimicrobial resistance could exacerbate these concerns.

- **Aging Population:** The average age of the general public is increasing (adults over the age of 65 composed 15.2% of the population in 2016 but are projected to make up more than 20% in 2030), which may increase the frequency at which emergency medical response is needed, potentially stressing available resources.

Communications

ESS operations are highly reliant on communications services and equipment to effectively execute mission functions. All manner of ES communications are susceptible to disruptions from natural hazards, cyberattacks, physical attacks, and general coverage and interference issues. With thousands of separate systems, networks, and equipment models, communications interoperability can be a major challenge between different ES organizations or disciplines. Increased adoption of digital and Internet technologies for ES communications adds cybersecurity concerns (see increased connectivity and disruptive digital technology in the Cybersecurity section above).

- **Communication Disruptions:** In large-scale response efforts, many additional resources supplement local organizations. Local emergency communication networks may not support the influx of traffic, resulting in busy signals and lack of available frequency. Additionally, the incident itself could affect communications infrastructure, reducing availability.
- **Interoperability Issues:** In recent years, public safety has seen a rapid expansion in technology advancements and in the type and manner of information sharing among responders and government officials. New applications and systems have created new challenges for interoperability and for ensuring the right people receive critical information at the right time.

Dependencies on Other Sectors

Both ES personnel and ES-related physical and cyber assets rely heavily on the resources and continual operation of other critical infrastructure sectors, including the Communications, Energy, Healthcare and Public Health, Information Technology, Transportation Systems, and Water and Wastewater Systems Sectors. In addition, the sector provides essential public-safety-related services to all other sectors, including both support for personnel and restoration of infrastructure on which the other sectors rely.

- **Communications:** As described above, the ESS heavily relies on operational and public communications, such as through an internal communications network, 9-1-1 services, or other public alerting and warning systems.
- **Energy:** Fuel and electrical power are essential for sustainment of ESS operations and supporting facilities.
- **Healthcare and Public Health:** In responding to emergencies, EMS and other first responders coordinate with the Healthcare Sector.
- **Information Technology:** Use of greater automation, CAD, watch and warning systems, and wearable sensors demonstrates ES disciplines' increasing dependence on digital assets and networks to carry out missions. Reliable IT improves services by providing essential support to ES personnel.
- **Transportation Systems:** To respond to emergencies effectively, the ESS depends on a resilient transportation network. Response vehicles must be able to transport people, goods, and services to and from incident areas. This includes the movement of ES assets to other geographical locations throughout the Nation.
- **Water and Wastewater Systems:** The critical mission of providing emergency services, such as in firefighting and public works, requires a clean and reliable water supply.

Case Study: Transporting Resources in Sandy's Wake

October 2012 brought one of the most destructive hurricanes in recent U.S. history. Hurricane Sandy caused unprecedented storm surges and flooding that devastated communities in 24 states, from the eastern seaboard west to Michigan and Wisconsin, as well as nations in the Caribbean, Bermuda, and Canada. In many areas, the private sector drew on lessons learned from past storms, implementing response and recovery successfully.

Nonetheless, Sandy presented significant challenges, exacerbated in part by transport difficulties, especially for utility crews and other first responders that had to cross state lines to support emergency response efforts. According to the *Regional Fleet Movement Coordination Initiative*, a one-hour delay in fleet movements can put restoration efforts back an entire day. The region was battling lost power and paralyzed fuel distribution networks, both of which caused cascading difficulties throughout the private sector, highlighting interdependencies between sectors that had previously gone unremarked. Lack of communication and transparency between public and private sectors made coordination difficult, compounding transport and assistance challenges.

Lessons learned in Sandy's aftermath included a clear need to facilitate private-sector fleet and resource movements efficiently while remaining in compliance with state and federal requirements. Recommendations include developing a multi-state informational database to facilitate fleet vehicle movement, establishing vehicle EZ Pass accounts for emergency fleet response, providing fleet operators with widely accepted documentation in lieu of national credentials, looking to fleets that are successful in moving easily across state lines (e.g., ambulances) for best practices, improving regional communications, and developing standardized rules for response efforts for consistency across regions.

Endnotes

[1] A. Reichard et al., "Occupational Injuries and Exposures among Emergency Medical Services Workers," *Prehospital Emergency Care* (January 2017)
[2] M. D. Weaver et al., "An observational study of shift length, crew familiarity, and occupational injury and illness in emergency medical services workers," *Occup Environ Med* (September 2015)
[3] B. Choi et al., "Twenty-four-hour work shifts, increased job demands, and elevated blood pressure in professional firefighters," *International Archives of Occupational and Environmental Health* (July 2016)
[4] Federal Emergency Management Agency (FEMA), U.S. Fire Administration, Firefighter Fatalities in the United States in 2017 (September 2018)
[5] SAMHSA, "First Responders: Behavioral Health Concerns, Emergency Response, and Trauma," Disaster Technical Assistance Center Supplemental Research Bulletin (May 2018)
[6] Centers for Disease Control and Prevention (CDC), National Institute for Occupational Safety and Health (NIOSH), Emergency Medical Services Workers: Injury Data (March 2018)
[7] H. M. Tiesman et al., "Nonfatal Injuries to Law Enforcement Officers: A Rise in Assaults," *American Journal of Preventive Medicine* (February 2018)
[8] CDC, NIOSH, Emergency Medical Service Workers: Injury Data (March 2018)
[9] Talos, "New VPNFilter malware targets at least 500K networking devices worldwide" (May 2018)
[10] McAfee Labs, Threats Report (April 2017)
[11] *The Register*, "World's biggest DDoS attack record broken after just five days" (March 2018)
[12] *Christian Science Monitor*, "911 TDOS near Phoenix, AZ spread over twitter" (March 2017)
[13] Varonis, The State of CryptoWall in 2018 (June 2016)
[14] Symantec, Internet Security Threat Report (April 2018)
[15] National Oceanic and Atmospheric Administration (NOAA), "Billion-Dollar Weather and Climate Disasters" (January 2018)
[16] U.S. Department of Agriculture (USDA), "Wildland Firefighter Smoke Exposure" (October 2013)
[17] Federal Bureau of Investigation (FBI), Law Enforcement Officers Killed & Assaulted, 2018 (LEOKA), Table 24: Law Enforcement Officers Feloniously Killed (Spring 2019)
[18] University of Maryland, Global Terrorism Database, Query for incidents between 2016-2018 in the United States targeting police (April 2019)
[19] *Wired*, "Above Devastated Houston, Armies of Drones Prove Their Worth" (September 2017)
[20] *The New York Times*, "A Closer Look at the Drone Attack on Maduro in Venezuela" (August 2018)
[21] American Society of Civil Engineers (ASCE), 2017 Infrastructure Report Card (March 2017)
[22] U.S. Department of Energy (DOE), Transforming U.S. Energy Infrastructures in a Time of Rapid Change: The First Installment of the Quadrennial Energy Review (April 2015)
[23] U.S. Energy Information Administration (EIA), "Major utilities continue to increase spending on U.S. electric distribution systems," *Today in Energy* (July 2018)
[24] EIA, "Utilities continue to increase spending on transmission infrastructure," *Today in Energy* (February 2018)
[25] American Water Works Association, State of the Water Industry Report (2018)

Appendix A. Resources

Key resources for this document are listed below in alphabetical order within each chapter topic. Entries without links are available from the Homeland Security Information Network – Critical Infrastructure (HSIN-CI) website. HSIN-CI is the primary system through which private-sector owners and operators, the U.S. Department of Homeland Security (DHS), and other federal, state, and local government agencies collaborate to protect the Nation's critical infrastructure. HSIN-CI provides real-time collaboration tools including a virtual meeting space, document sharing, alerts, and instant messaging at no charge. Visit www.dhs.gov/hsin-critical-infrastructure for more information.

Operational Hazards

CDC, NOISH, Emergency Medical Workers (March 2018)
https://www.cdc.gov/niosh/topics/ems/default.html

CDC, NIOSH, Emergency Medical Services Workers: Injury Data (March 2018)
https://www.cdc.gov/niosh/topics/ems/data.html

CDC, NOISH, Firefighter Resources (August 2018) https://www.cdc.gov/niosh/firefighters/

Choi, B., Schnall, P., and Dobson, M., "Twenty-four-hour work shifts, increased job demands, and elevated blood pressure in professional firefighters," *International Archives of Occupational and Environmental Health* (July 2016) https://www.ncbi.nlm.nih.gov/pubmed/27368424

DHS, Project Responder 5 (August 2017) https://www.dhs.gov/sites/default/files/publications/Project-Responder-5-Report_170814-508.pdf

FBI, Law Enforcement Officers Killed and Assaulted (LOEKA) Program
https://www.fbi.gov/services/cjis/ucr/leoka

FEMA, Firefighter Fatalities in the United States in 2017 (September 2018)
https://www.usfa.fema.gov/downloads/pdf/publications/ff_fat17.pdf

FEMA, Risk Management Practices in the Fire Service (January 2018)
https://www.usfa.fema.gov/downloads/pdf/publications/risk_management_practices.pdf

International Committee of the Red Cross, Chemical, Biological, Radiological, and Nuclear Response Introductory Guidance (March 2014) https://www.icrc.org/en/publication/4175-chemical-biological-radiological-and-nuclear-response-introductory-guidance

Reichard, A., Marsh, S., Tonozzi, T., Konda, S., & Gormley, M., "Occupational Injuries and Exposures among Emergency Medical Services Workers," *Prehospital Emergency Care* (January 2017)
https://www.ncbi.nlm.nih.gov/pubmed/28121261

SAMHSA, "First Responders: Behavioral Health Concerns, Emergency Response, and Trauma," Disaster Technical Assistance Center Supplemental Research Bulletin (May 2018)
https://www.samhsa.gov/sites/default/files/dtac/supplementalresearchbulletin-firstresponders-may2018.pdf

Taylor, J. A., Barnes B., Davis A. L., Wright J., Widman S., and LeVasseur M., "Expecting the unexpected: A mixed methods study of violence to EMS responders in an urban fire department," *Am J Ind Med* (January 2016) https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4736678/

Tiesman, H. M. et al., "Nonfatal Injuries to Law Enforcement Officers: A Rise in Assaults," *American Journal of Preventive Medicine* (February 2018) https://www.ncbi.nlm.nih.gov/pubmed/29395571

Weaver, M. D., Patterson, P. D., Fabio, A., Moore, C. G., Freiberg, M. S., and Songer, T.J., "An observational study of shift length, crew familiarity, and occupational injury and illness in emergency medical services workers, *Occup Environ Med* (September 2015) https://www.ncbi.nlm.nih.gov/pubmed/26371071

Zagorski, Nick, "Study of 9/11 Responders Continues to Unveil New Information on PTSD," *Psychiatric News* (October 2016) https://psychnews.psychiatryonline.org/doi/full/10.1176/appi.pn.2016.10a25

Cybersecurity

Cisco, 2018 Annual Cybersecurity Report (February 2018) https://www.cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html

Cyber Threat Alliance, Lucrative Ransomware Attacks: Analysis of the CryptoWall Version 3 Threat (October 2015) https://www.cyberthreatalliance.org/wp-content/uploads/2018/02/cryptowall-report.pdf

DHS, Cloud Security Guidance (February 2018) https://www.us-cert.gov/sites/default/files/publications/Cloud_Security_Guidance-.gov_Cloud_Security_Baseline.pdf

DHS, Cyber Risks to Next Generation 9-1-1 (November 2018) https://www.dhs.gov/sites/default/files/publications/Cybersecurity Risks for NG9-1-1 (100418)_508C_FINAL.pdf

DHS, Cyber Techniques and Possible Impacts of Activity Against the Emergency Services Sector (January 2019)

DHS Office of Intelligence and Analysis (I&A), Preliminary Analysis of Attacks in 2017 Highlight Threat to Uniformed Personnel, Exploitation of Public Spaces to Target Civilians (May 2017)

DHS Office of Cyber and Infrastructure Analysis (OCIA), Cybersecurity Risks Posed by Unmanned Aircraft Systems (May 2018)

DHS OCIA, Ransomware: Goals of Malicious Actors and Current System Vulnerabilities (June 2017)

DHS OCIA, Potential Impacts of WannaCry Ransomware on Critical Infrastructure (May 2017)

DHS OCIA, Risks to Critical Infrastructure that Use Cloud Services (June 2017)

DHS Science and Technology Directorate (S&T), Distributed Denial of Service Defense https://www.dhs.gov/science-and-technology/ddosd

DHS S&T, Telephony Denial of Service Factsheet (2014) https://www.dhs.gov/sites/default/files/publications/508_FactSheet_DDoSD_TDoS One Pager-Final_June 2016_0.pdf

National Institute of Standards and Technology, Draft NISTIR 8196: Security Analysis of First Responder Mobile and Wearable Devices (December 2018) https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8196-draft.pdf

Sternstein, Aliya, "How Homeland Security plans to end the scourge of DDoS attacks," *The Christian Science Monitor* (March 2017) https://www.csmonitor.com/World/Passcode/2017/0308/How-Homeland-Security-plans-to-end-the-scourge-of-DDoS-attacks

Symantec, Internet Security Threat Report (April 2018) https://www.symantec.com/security-center/threat-report

U.S. Computer Emergency Readiness Team (US-CERT), Alert (TA18-201A) Emotet Malware (July 2018) https://www.us-cert.gov/ncas/alerts/TA18-201A

Varonis, "The State of CryptoWall in 2018" (June 2016) https://www.varonis.com/blog/cryptowall/

Natural Hazards

CDC, NIOSH, Fighting Wildfires (May 2018) https://www.cdc.gov/niosh/topics/firefighting/default.html

DHS OCIA, Pandemic Impacts to Lifeline Critical Infrastructure (July 2015)

DHS OCIA, Tropical Storm Harvey: Infrastructure Impact Summary (August 2017)

DHS OCIA, 2017 Wildland Fires and Potential Effects to Critical Infrastructure (June 2017)

DHS Office of Infrastructure Protection (OIP), Current Situation Report: California Fires – Multiple Counties, CA – 11 Oct 17 (Update 03)

U.S. Chemical Safety Board, Organic Peroxide Decomposition, Release, and Fire at Arkema Crosby Following Hurricane Harvey Flooding. Report Number: 2017-08-I-TX (May 2018) https://www.csb.gov/arkema-inc-chemical-plant-fire-/

USDA, Wildland Firefighter Smoke Exposure (October 2013) https://www.fs.fed.us/t-d/pubs/pdfpubs/pdf13511803/pdf13511803dpi100.pdf

Criminal Activities and Terrorism

Combating Terrorism Center at West Point, Lessons Learned from the Police Response to the San Bernardino and Orlando Terrorist Attacks (May 2017) https://ctc.usma.edu/lessons-learned-from-the-police-response-to-the-san-bernardino-and-orlando-terrorist-attacks/

DHS, Emergency Response Vehicle and Equipment Security (October 2015)

DHS, Unmanned Aircraft Systems: Addressing Critical Infrastructure Security Challenges (February 2017) https://www.dhs.gov/sites/default/files/publications/uas-ci-challenges-fact-sheet-508.pdf

DHS, Unmanned Aircraft Systems: Considerations for Law Enforcement Action (June 2017) https://www.dhs.gov/sites/default/files/publications/uas-law-enforcement-considerations-508.pdf

DHS, Illicit Unmanned Aircraft Encounters Continue to Rise in Florida, Likely Increasing Demand on Law Enforcement Response (January 2017)

DHS OCIA, Preliminary Analysis of Attacks in 2017 Highlight Threat to Uniformed Personnel, Exploitation of Public Spaces to Target Civilians (September 2017)

FBI, Law Enforcement Officers Killed & Assaulted, 2018 (LEOKA) (Spring 2019) https://ucr.fbi.gov/leoka/2018/home

National Interagency Fire Center, Drones and Wildfires (accessed 2019) https://www.nifc.gov/drones/outreach.html

Medina, Jennifer, "Chasing Video with Drones, Hobbyists Imperil California Firefighting Efforts," *The New York Times* (July 2015) https://www.nytimes.com/2015/07/20/us/hobby-drones-hinder-california-firefighting-efforts.html

Marshall, Aarian, "Above Devastated Houston, Armies of Drones Prove Their Worth," *Wired* (September 2017) https://www.wired.com/story/houston-recovery-drones/

Crosscutting Issues

American Water Works Association, State of the Water Industry Report (2018) https://www.awwa.org/Portals/0/AWWA/Development/Managers/2018_SOTWI_Report_Final_v3.pdf

ASCE, 2017 Infrastructure Report Card (March 2017)

DHS, Crisis Event Response and Recovery Access (CERRA) Framework: An Emergency Preparedness Access Implementation and Best Practice Guide https://www.dhs.gov/sites/default/files/publications/Crisis Event Response and Recovery Access (CERRA) Framework.pdf

DOE, Transforming U.S. Energy Infrastructures in a Time of Rapid Change: The First Installment of the Quadrennial Energy Review (April 2015) https://www.energy.gov/sites/prod/files/2015/08/f25/QER Summary for Policymakers April 2015.pdf

EIA, "Major utilities continue to increase spending on U.S. electric distribution systems," *Today in Energy* (July 2018) https://www.eia.gov/todayinenergy/detail.php?id=36675

EIA, "Utilities continue to increase spending on transmission infrastructure," *Today in Energy* (February 2018) https://www.eia.gov/todayinenergy/detail.php?id=34892

Multi-State Fleet Response Working Group (FRWG), Regional Fleet Movement Coordination Initiative Overview (August 2015) http://www.fleetresponse.org/wp-content/uploads/sites/2/2014/07/Fleet_Movement_Coordination_Inititiative_Info_packet_7_3_2014.pdf

National Homeland Security Consortium, 2016 National Issues Brief (March 2016) https://www.nemaweb.org/nhsc/index.html

Appendix B. Tools, Training, and Programs

Relevant tools, training, programs, and Emergency Services Sector publications that may help sector stakeholders address the security and resilience issues described in this document are listed below. These resources are organized by alphabetical order within each chapter topic. This listing is not exhaustive, but it provides key resources sector stakeholders may find useful.

Operational Hazards

Emergency Services Sector – Continuity Planning Suite (ESS-CPS) – The ESS-CPS provides a centralized collection of existing guidance, processes, products, tools, and best practices to support the development and maturation of continuity planning for the first responder community. The ESS-CPS was created through a partnership of the Emergency Services Sector-Specific Agency (SSA) and Sector Coordinating Council (SCC). First responders can use the ESS-CPS as it suits their organizations to evaluate and improve their continuity capability and enhance their preparedness for emergencies. https://www.dhs.gov/emergency-services-sector-continuity-planning-suite

IS-454: Fundamentals of Risk Management – This course is designed to foster an overall culture of risk management throughout the DHS workforce. While providing awareness of the fundamental concepts of risk management, the course will prepare employees to manage risk at home, in the workplace, and the community and provide them with a foundation for further development in the area of risk management.

IS-906: Workplace Security Awareness – This course provides guidance to individuals and organizations on how to improve workplace security. No workplace—be it an office building, construction site, factory floor, or retail store—is immune from security threats.

Cybersecurity

Emergency Services Sector Cybersecurity Best Practices – This fact sheet assists ES organizations and personnel with better protecting themselves by implementing some simple, effective, low-cost measures. In addition to general cybersecurity practices, it also addresses best practices for social networking, email, Wi-Fi, and Bluetooth. https://www.dhs.gov/publication/emergency-services-sector-cybersecurity-initiative

Emergency Services Sector – Cyber Risk Assessment (ESS-CRA) – The ESS-CRA is the first sector-wide assessment that analyzes strategic cyber risks to ES infrastructure. The ESS-CRA results help the sector understand and manage cyber risks and provide a national-level risk profile that ES organizations can use to prioritize how they spend resources and where to focus training, education, equipment investments, grant requests, and further study. https://www.dhs.gov/publication/emergency-services-sector-cybersecurity-initiative

Emergency Services Sector Roadmap to Secure Voice and Data Systems – The follow-up to the ESS-CRA, this roadmap identifies and discusses proposed risk mitigation measures to address the risks identified in the ESS-CRA. https://www.dhs.gov/publication/emergency-services-sector-cybersecurity-initiative

Cyber Resilience Review (CRR) – The Cyber Security Evaluation Program conducts no-cost, voluntary CRRs to evaluate and enhance cybersecurity capacities and capabilities within all 16 critical infrastructure sectors, as well as state, local, tribal, and territorial governments. The CRR seeks to understand cybersecurity critical for an organization's success by focusing on protection and sustainment practices within ten key domains that contribute to an organization's overall cyber resilience. https://www.us-cert.gov/ccubedvp/assessments

Natural Hazards

Hazus – Hazus is a nationally applicable standardized methodology that estimates potential losses from earthquakes, hurricane winds, floods, and tsunamis. Hazus can assist mitigation planning teams with understanding vulnerabilities and describing impacts in the hazard identification and risk assessment portion of their mitigation plans. Hazus can generate loss estimates with its default data, but it can also be used in combination with local information to generate more refined loss estimates.
https://www.fema.gov/hazus

Using Hazus for Mitigation Planning – This job aid helps mitigation planners better leverage Hazus data, maps, and tables in their hazard mitigation plans. https://www.fema.gov/media-library-data/1540479624999-ab1eca852448e271f0de82cf2031a01b/Using_Hazus_in_Mitigation_Planning_20180820_Final_508_Compliant.pdf

Criminal Activities and Terrorism

Introduction to the Terrorist Attack Cycle (AWR-334) – This course introduces a conceptual model of common steps that terrorists take in planning and executing terrorist attacks. It enhances participants' awareness and capability of preventing, protecting against, responding to, and mitigating attacks that use improvised explosive devices against people, critical infrastructure, and other soft targets.
https://cdp.dhs.gov/find-training/course/AWR-334

Response to Suspicious Behaviors and Items (AWR-335) – This course serves as an overview of appropriate responses to suspicious behaviors and items by differentiating normal and abnormal behaviors and highlighting appropriate responses to potential terrorist or criminal activity. The course also discusses the differences between unattended and suspicious items and the responses for each situation.
https://cdp.dhs.gov/find-training/course/AWR-335

Suspicious Activity Reporting (SAR) Explosive Precursors Point of Sale Training – The Nationwide SAR Initiative (NSI) offers this interactive course to instruct sales personnel involved at the point of sale on behaviors and indicators that are reasonably indicative of potential terrorist and/or criminal bomb-making activity; how and where to report suspicious activity; and how to protect privacy, civil rights, and civil liberties when documenting information. The course also instructs personnel about the types of suspicious activity that might be observed during their daily duties.
https://nsi.ncirc.gov/hsptregistration/explosive_precursors/

Suspicious Activity Reporting (SAR) Training for Law Enforcement and Hometown Security Partners – The NSI offers online interactive courses for frontline officers and hometown security partners to recognize behaviors and indicators that, depending on the context of the observation, may indicate terrorism-related criminal activity. These trainings also discuss how to report identified suspicious activity to the proper authorities while maintaining the protection of citizens' privacy, civil rights, and civil liberties.
https://nsi.ncirc.gov/training_online.aspx

Crosscutting Issues

Crisis Event Response and Recovery Access (CERRA) Framework: An Emergency Preparedness Access Implementation and Best Practice Guide – The CERRA Framework focuses on supporting state, local, and regional efforts to enable the successful transit and access of critical response and recovery resources before, during, and after emergencies. https://www.dhs.gov/publication/crisis-event-response-and-recovery-access

Incident Management Preparedness and Coordination Toolkit (IMPACT) – IMPACT is a free all-hazards planning tool for first responders. It is meant to augment, not replace, current tools first responders may already be using. IMPACT combines simulation, visualization, and mapping into an integrated user interface similar to a smart phone or tablet. First responders can use it for planning, situation awareness, and response to natural and man-made disasters. It uses common data formats so that data is easily exchanged with other map-based tools. https://geo.ornl.gov/impact/index.html

Interoperable Communications Technical Assistance Program (ICTAP) – ICTAP serves all 56 states and territories and provides direct support from CISA to state, local, and tribal emergency responders and government officials through the development and delivery of training, tools, and onsite assistance to advance public safety interoperable communications capabilities. https://www.dhs.gov/cisa/interoperable-communications-technical-assistance-program

National Council of Statewide Interoperability Coordinators (NCSWIC) – Established by CISA, NCSWIC supports Statewide Interoperability Coordinators (SWIC) from the 56 states and territories, by developing products and services to assist them with leveraging their relationships, professional knowledge, and experience with public safety partners involved in interoperable communications at all levels of government. https://www.dhs.gov/safecom/NCSWIC

S&T First Responders – The DHS Science & Technology Directorate (S&T) works with first responders across all disciplines to understand challenges, needs, and requirements and to develop capabilities that improve safety of first responders. S&T strengthens first responder capabilities in daily operations and in response to critical incidents and catastrophic events and modern criminal investigations. https://www.dhs.gov/science-and-technology/first-responders

SAFECOM – Through collaboration with emergency responders and elected officials across all levels of government, SAFECOM (managed by CISA) works to improve emergency response providers' inter-jurisdictional and interdisciplinary emergency communications interoperability across local, regional, tribal, state, territorial, international borders, and with federal government entities. SAFECOM works with existing federal communications programs and key emergency response stakeholders to address the need to develop better technologies and processes for the coordination of existing communications systems and future networks. https://www.dhs.gov/safecom#