EMERGENCY SERVICES SECTOR

ROADMAP TO SECURE VOICE AND DATA SYSTEMS

November 2023

Cybersecurity and Infrastructure Security Agency

CONTENTS

EMERGENCY SERVICES SECTOR COORDINATING COUNCIL / GOVERNMENT COORDINATING COUNCIL MEMORANDUM OF COORDINATION

The complexity of the Emergency Services Sector (ESS), along with its unique mission to protect the public and the other 15 Critical Infrastructure sectors, creates unique challenges in developing and implementing a risk management approach. The Emergency Services Government Coordinating Council (GCC) and Sector Coordinating Council (SCC) believe that 'protecting the protectors' is critical, and are dedicated to working with the community to ensure the protection of its infrastructure, and first and foremost, its personnel.

In 2011, through the Critical Infrastructure Partnership Advisory Council framework, the ESS committed to the completion of a sector-wide cyber risk assessment. The 2012 *Emergency Services Sector Cyber Risk Assessment* (*ESS CRA*) is the first ESS-wide cyber risk assessment completed under the National Infrastructure Protection Plan framework, and it will inform collaborative and synchronized management of cyber risk across the sector.

The *ESS CRA* is the initial effort to assess ESS cyber risks across the ESS disciplines and serves as a baseline of national-level risk. The assessment addresses those operational or strategic risks to the ESS infrastructure that are of national concern based upon the knowledge and collaboration of subject matter experts participating in the sector's risk assessment activities. Within the *ESS CRA*, the following occurred:

- Sector disciplines, value chains, and associated cyber infrastructure for assessment were verified;
- Seven cyber risk scenarios were developed and applied across multiple ESS disciplines;
- ESS risks within the cyber risk scenarios were identified;
- Threats, vulnerabilities, and consequences inherent in ESS risks were evaluated; and
- Risks within ESS disciplines were aggregated to create an ESS risk profile.

To address the cyber risks identified in the *ESS CRA*, the ESS Cyber Working Group, in conjunction with the U.S. Department of Homeland Security National Protection and Programs Directorate's Industry Engagement and Resilience Branch within the Stakeholder Engagement and Cyber Infrastructure Resilience Division of the Office of Cyber Security and Communications and the Emergency Services Sector Management Team within the Sector Outreach and Programs Division of the Office of Infrastructure Protection, developed the *Emergency Services Sector Roadmap to Secure Voice and Data Systems* (*Roadmap*).

The *Roadmap* identifies and discusses several proposed risk mitigation measures and includes justification for the response, sector context, barriers to implementation, and suggestions for implementation. The Roadmap is intended to serve as a guide and reference document for ESS personnel as they adapt to the growing prevalence of and reliance upon digital technologies and other cyber infrastructure in the sector. The ESS Cyber Working Group will revisit the results from the *ESS CRA* and the *Roadmap* on a continual basis to identify emerging cyber risks, cyber incident trends, and other cybersecurity issues for sector collaboration.

By signing this letter, the Emergency Services GCC and SCC commit to:

- Consider Roadmap analyses and findings, and carry out our assigned functional responsibilities regarding the management of ESS cyber risks as described herein;

- Work with the Secretary of Homeland Security as the Emergency Services Sector Risk Management Agency, as appropriate and consistent with GCC and SCC member-specific authorities, resources, and programs, to coordinate funding and implementation of programs that effectively manage ESS cyber risks;
- Cooperate and coordinate with the Secretary of Homeland Security as the Emergency Services Sector Risk Management Agency, in accordance with guidance provided in Presidential Policy Directive-21: Critical Infrastructure Security and Resilience (which replaced Homeland Security Presidential Directive - 7), as appropriate and consistent with GCC and SCC member-specific authorities, resources, and programs, to facilitate management of ESS cyber risks;
- Develop and/or modify existing inter- and intra-agency cyber risk management plans/roadmaps, as appropriate, to facilitate compliance with the Emergency Services Sector-Specific Plan;
- Develop and maintain partnerships for ESS cyber risk management with appropriate state, regional, local, tribal, territorial and international entities; private sector owners, operators, and associations; and nongovernmental organizations; and
- Protect critical infrastructure information according to the Protected Critical Infrastructure Information Program or other appropriate guidelines, and share ESS cyber risk management information, as appropriate and consistent with GCC and SCC member-specific authorities and the process described herein.

The *ESS CRA* describes an effort that requires resources and coordination from across all disciplines of the ESS in order to assess cyber risks to ESS critical infrastructure. This risk assessment provides the basis for the *Roadmap* that will ensure that Federal resources are applied where they offer the most benefit for mitigating risk by deterring threats, limiting vulnerabilities, and minimizing the consequences of attacks and other incidents, and encourages a similar risk-based allocation of resources within state, local, tribal, and territorial entities and the private sector.

Signatories

Tonya Schreiber
Director, Sector Outreach and Programs Division
Office of Infrastructure Protection
National Protection and Programs Directorate
U.S. Department of Homeland Security

Dan Schultz
Chief, Emergency Services Sector-Specific Agency
Chair, Emergency Services GCC

Signatories

Shawn Kelley
International Association of Fire Chiefs
Chair, Emergency Services SCC

Mark Hogan
City of Tulsa, Oklahoma
Chair, ESS Cyber Working Group

EXECUTIVE SUMMARY

In 2011, the Emergency Services Sector (ESS) Cyber Working Group developed a draft cybersecurity roadmap to help Federal, state, local, tribal, and territorial governments, as well as contract non-governmental organizations and agencies in law enforcement, fire and emergency services, emergency medical services, emergency management, and public works disciplines, consider and act on the emerging threats that they were beginning to face in cyberspace. Consequently, the Cyber Working Group teamed with staff from the U.S. Department of Homeland Security's (DHS) Industry Engagement and Resilience (IER) Branch (previously part of the former National Cyber Security Division) to further explore and build an understanding of cyber risks and the nature of the cyber threats that ESS agencies were facing.

Through that collaborative effort, DHS and the ESS Cyber Working Group decided to postpone the draft cybersecurity roadmap and first conducted a sector-wide strategic-level evaluation of cyber risks facing the sector. This evaluation resulted in the *Emergency Services Sector Cyber Risk Assessment* (*ESS CRA*), published in April 2012.[1] The focus of that assessment was to identify the most likely threat scenarios that ESS agencies may face when using their cyber resources, which include voice, data, and video communications systems over both wired and wireless networks. Following the publication of the *ESS CRA*, the Cyber Working Group decided to reshape the previous version of the cybersecurity roadmap to identify risk responses for each of the cyber risks identified in the *ESS CRA*. This document, the *Emergency Services Sector Roadmap to Secure Voice and Data Systems*, (hereafter the *Roadmap*) represents that collection of cyber risk response strategies.

The Cyber Working Group met in five sessions to carefully consider the cyber risks identified in the *ESS CRA* and, in collaboration with IER staff, to develop cyber risk mitigation measures to address those risks. The identified risk mitigation measures are intended to mitigate cyber risks, either by reducing the likelihood that a risk could be realized, by reducing the consequences of a cyber incident that actually occurs, or both. It is important to note that while these measures were developed in response to the scenarios used in the *ESS CRA*, they may be applicable to more than one scenario and may offer additional risk reduction for scenarios not yet considered by the Cyber Working Group.

The *Roadmap* discusses each proposed risk mitigation measure and includes justification for the response, sector context, barriers to implementation, and suggestions for implementation. Table 1 on page 2 provides a summary of the identified cyber risk mitigation measures and the extent to which ESS personnel may need Federal Government assistance or engagement to implement a given cyber risk mitigation or the level of Federal assistance available to implement a cyber risk mitigation measure. However, it is evident to a great extent that addressing cyber risks in the ESS is the role and responsibility of each agency, regardless of discipline. There may be Federal resources available to provide insights or assistance, but addressing cyber risk is a job for each agency to address.

[1] For a copy of the *ESS CRA*, contact the Emergency Services Sector Management Team at EmergencyServicesSector@cisa.dhs.gov or visit the HSIN-ES or HSIN-CI Website.

Table 1. Summary of Recommended Cyber Risk Mitigation Measures

Cyber Risk Mitigation Measure	Federal Influence or Engagement	More Information
Adopt and Implement Next Generation 9-1-1 Services	Heavy	Page 18
Create and Implement an Alternative Emergency Number to 9-1-1 and/or Expand the Number of Available 9-1-1 Trunk Lines	Little or None	Page 25
Create Alternate Emergency Operation Centers and Additional Public Safety Answering Point Facilities	Little or None	Page 29
Create Diversity in Public Safety Answering Point and Communications Infrastructure Facilities	Little or None	Page 32
Implement Improved Physical Security Measures at Public Safety Answering Point and Communications Infrastructure Facilities	Little or None	Page 36
Adopt and Implement Rollover Capabilities in Public Safety Answering Point and Emergency Operation Center facilities	Little or None	Page 41
Conduct and Evaluate Failover Capabilities through Exercises	Little or None	Page 46
Establish Comprehensive Cybersecurity and Continuity of Operations Plan Implementation Training and Education for Staff	Moderate	Page 48
Create Hot Continuity of Operations Sites with Database Backups	Little or None	Page 53
Evaluate the Use of Amateur Radio Networks, Talk-Around Channels, and Talk Groups and Establishing an Area Command to Manage Consequences of Incidents	Little or None	Page 57
Implement Public Alerting and Warning Systems to Provide Guidance for the Public	Little or None	Page 62
Adopt and Implement Security Policies and Procedures to Protect Sector Databases and Public Alerting and Warning Systems	Little or None	Page 64
Implement Standards, Guidelines, and Best Practices for Surveillance Technologies and Capabilities	Little or None	Page 72
Evaluate the Physical Location of Cameras and Other Surveillance Technologies	Little or None	Page 74
Implement Artificial Intelligence to Assist with Monitoring and Tracking Potential Risks	Little or None	Page 77

These 15 cyber risk mitigation measures are accompanied by recommendations of actions necessary to develop and implement them. Each section includes notional recommendations of the key officials who can lead and influence development and implementation, primary leadership or organizations that should pursue development and implementation, and the supporting organizations that can help facilitate the implementation.

The *Roadmap* is intended to serve as a guide and reference document for ESS personnel as they adapt to the growing prevalence of and reliance upon digital technologies and other cyber infrastructure in the sector. The ESS Cyber Working Group will revisit the results from the *ESS CRA* and the *Roadmap* on a continual basis to identify emerging cyber risks, cyber incident trends, and other cybersecurity issues for sector collaboration.

INTRODUCTION

The U.S. Department of Homeland Security (DHS) in conjunction with the Office of Infrastructure Protection Emergency Services Sector (ESS) Government Coordinating Council and Sector Coordinating Council's Cyber Working Group conducted the first risk assessment of the sector's cyber resources in 2011. This effort was consistent with the ESS Sector-Specific Plan, an annex to the National Infrastructure Protection Plan that was developed for the Emergency Services Sector in 2010. The ESS vision, as stated in the *Emergency Services Sector-Specific Plan*, is:

> An Emergency Services Sector in which facilities, key support systems, information and coordination systems, and personnel are protected from both ordinary operational risks and from extraordinary risks or attacks, ensuring timely, coordinated, all-hazards emergency response and public confidence in the sector.

The first step in fulfilling this vision from a cyber risk standpoint was to conduct the *Emergency Services Sector Cyber Risk Assessment* (*ESS CRA*). That effort was conducted using the Cybersecurity Assessment and Risk Management Approach (CARMA), which is composed of five stages as shown below:

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

This Roadmap represents Stage IV activities. By following the five stages, the Emergency Services Sector has made significant progress in completing the initial approach:

Stage I Scope Risk Management Activities: COMPLETED
Documented in the ESS CRA

Stage II Identify Cyber Infrastructure: COMPLETED
Documented in the ESS CRA

Stage III Conduct Cyber Risk Assessment: COMPLETED
Documented in the ESS CRA

Stage IV Develop Cyber Risk Management Strategy: COMPLETED
Documented in this Roadmap

Stage V Implement Strategy and Measure Effectiveness: NOT STARTED

The results of the first three CARMA stages were published in the *ESS CRA* in 2012. The assessment, conducted using seven scenarios identified by the Cyber Working Group as threats to the cyber resources on which the sector relies to accomplish its mission, addressed the first three stages of the CARMA framework. This *Emergency Services Sector*

Roadmap to Secure Voice and Data Systems (hereafter the *Roadmap*) represents the culmination of Stage IV. It was developed in collaboration with DHS and the members of the ESS Cyber Working Group, which convened again in 2012 to identify a strategy and activities in response to the *ESS CRA*.

While the *ESS CRA* was conducted using threat-based scenarios to determine risks and vulnerabilities that the sector faces, responses to those threats were seen as applicable to an array of threats far beyond those identified for the assessment. Thus, this *Roadmap* presents a strategy and activities that, when implemented, will provide a much broader level of cyber risk mitigation and protection than that required to address the seven scenarios identified in the *ESS CRA*.

In this document, ESS organizations will find the next steps they should take based on *ESS CRA* and CARMA Stage IV activities to mitigate cyber risks. Each mitigation is introduced, is associated with the cyber risk it is intended to mitigate, and is presented in terms of its estimated impact (or expected reduction of cyber risks) and its implementation feasibility or challenges.

In a familiar format, this *Roadmap* provides the ESS with actionable mitigation activities that sector disciplines can pursue to support the cyber risk strategy. Every day across the United States, the ESS organizes and executes its response activities in a manner consistent with the National Response Framework (NRF) and the National Incident Management System (NIMS). The *Roadmap's* strategy was developed as a risk response to cyber threats. To support risk response using that doctrine, the *Roadmap* is presented in a manner consistent with the NRF and NIMS. In terms similar to those used in the Incident Command System (ICS) section of the NRF, the *Roadmap* identifies the coordination needed, the primary parties recommended to address the mitigation activity, and the supporting parties recommended to engage in implementation. Many ESS organizations have internal divisions or bureaus loosely aligned with the four main sections of ICS, Operations, Logistics, Planning, and Administration/Finance. The *Roadmap* was developed to follow this ICS model to help key authorities and decision-making groups quickly discern how to divide the responsibilities for each mitigation measure.

Thus, the primary and supporting parties are also identified as those responsible for the four primary sections/responsibilities identified in NIMS—Operations, Planning, Logistics, and Administration/Finance. This means of presenting the *Roadmap* should help the sector's organizational leaders determine roles, responsibilities, and timeframes required to implement its recommended strategies.

CYBER RISK STRATEGY FOR THE ESS

The *Roadmap* assumes four means of addressing risk:

- **Avoidance**—Activities that eliminate or withdraw from exposure to risks. Avoidance activities commonly include identifying, assessing, and prioritizing risks and then using available resources (such as training, policies, practices, and procedures) to minimize the probability or impact of a threat or incident occurring. Risk avoidance occurs when a sector or an entity either makes a decision to not operate in a certain way because of its inherent risk or chooses another operating method that inherently has less risk. To avoid in the context of an emerging threat or risk is to avoid vulnerability through alternate technology or process revision. Examples include deciding not to adapt an emerging technology or deploying an innovation or updated technology based on an identified risk. A follow-on risk assessment should be conducted to see if the overall risk to the sector outweighs the avoidance strategy. Avoiding a risk includes taking steps to engage in an alternative activity (such as selecting one technology or process over another) or otherwise ending an exposure to eliminate the vulnerability.
- **Mitigation**—Activities to optimize resilience against risks. These activities are systematic approaches to reducing exposure or the extent of exposure to a risk or to an incident that actually occurs. Systematic approaches may include automated risk monitoring or enhanced security measures. Mitigating risk occurs through the implementation of protective programs or through research and development (R&D). Sector threats will be updated regularly and compared to sector protective programs and R&D initiatives to identify new areas to pursue and new research to mitigate threats to sector critical functions.
- **Transference**—Transferring risks to others, either by means that outsource risks to other organizations or insuring against the consequences of an incident that actually occurs. Transferring and sharing risks is a regular occurrence in the ESS due to the shared roles and responsibilities different ESS organizations play during response and recovery activities. Transferring a risk could be considered a feasible option to supplement mitigations or as a standalone strategy when other risk response efforts are ineffective. Transferring risk most commonly occurs through the purchase of insurance, whereby an entity shares the risk with another. Recent developments include using a range of risk transfer mechanisms, such as catastrophe bonds, catastrophe pools, and index-based insurance, and micro-insurance schemes.
- **Acceptance**—Retaining and accepting the risks inherent to an organization's business and budgeting resources to address losses that may be incurred if a threat or incident is realized. ESS organizations retain certain risks on a daily basis as the cyber resources upon which they rely are often regarded as essential tools to executing their missions. Yet, like any tool, they are subject to damage or failure from misuse, abuse, wear, and obsolescence. Accepting the risk means that the sector does not assume that it requires further reduction. Although accepting a risk is considered passive and easy to implement regarding cost and time, there are other feasibility costs associated with implementing this strategy. Repeated assessment and measurement of the risk is necessary, as accepting risk may not be effective or feasible if it becomes of greater concern.

ESS organizations encounter many physical risks while delivering services; they also face cyber risks daily in a number of forms. This *Roadmap* draws from the *ESS CRA* results in

developing a strategy to address them. In most instances, the sector's strategy to date has been to accept risks to its cyber resources. However, the development of technologies that allow greater communications, collaboration, and cooperation among the sector disciplines—law enforcement, fire and emergency services, emergency medical services, emergency management, and public works; and two additional disciplines, public safety communications and public safety coordination and fusion—have created new risks that require a more systematic and strategic response than ever before.

While acknowledging that acceptance is a commonly practiced means of addressing cyber risk, the *Roadmap* strives to detail the full range of risk response options to provide for greater protection. While beyond the scope of this report to categorize recommended risk mitigation activities to support this strategy, each can be aligned with one of these four accepted means of risk management.

RECOMMENDED RISK MITIGATION MEASURES

In the remainder of the *Roadmap*, the risk mitigation measures identified by the ESS Cyber Working Group are presented in five segments:

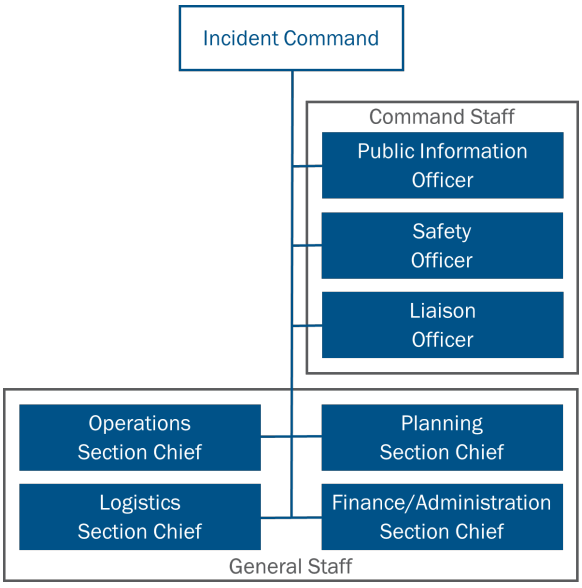
1. Preserving and Protecting Citizen Access to Emergency Services
2. Protecting Facility and Cyber Infrastructure Capabilities
3. Planning and Preparing for Cyber Incidents
4. Using and Assuring Public Alerting and Warning Systems
5. Defending Surveillance Systems and Networks.

Each segment includes specific risk mitigation measures along with their background or history. Overviews of these measures include descriptions of the recommended activities necessary to reduce cyber risk. The ESS Cyber Working Group evaluated each measure to discern the effect it may have on cyber risks (or, to what extent is cyber risk reduced) and on any known challenges (the feasibility of the measure) in its implementation.

These measures are not presented in the scenario-based risks identified in the *ESS CRA*; they have been determined to have a broader application and provide a greater means of reducing risk beyond threats identified in that report.

The ESS strategy for adopting and implementing the risk mitigation measures provided in this *Roadmap* is to use the organizational structure of the NIMS, which uses a common Incident Command System (ICS) to promote effective and efficient incident response and recovery operations. While a cyber threat may evolve into an actual incident, this *Roadmap* offers the organizational construct of ICS as a means of designating roles and responsibilities in developing the recommended risk mitigations measures. A key leader or leadership group will oversee the adoption and implementation of the recommended cyber risk mitigation measures. Figure 1 below shows the ICS organization found in NIMS.

Figure 1. Incident Command System Organizational Structure.



The Roadmap uses the four General Staff Section Chief positions to represent responsibilities for implementing risk mitigation measures. Each section would report to a

key authority or leadership group overseeing the adoption and implementation of each cyber risk mitigation measure.

While a key authority or group will oversee the adoption and implementation of the cyber risk mitigation measures, each measure in this *Roadmap* also includes a recommendation for which of the sections should take the lead and which should support the lead in implementation. The term "section" can be substituted with department or agency if cyber resources and/or services are furnished by an outside department or agency that would otherwise handle such activities.

The primary section roles, excerpted and modified from the NIMS, are defined as follows:

- **Operations**-Operations Section is responsible for all tactical activities focused on reducing the immediate hazard, establishing situational control, and restoring normal operations.
- **Planning**-Planning Section collects, evaluates, and disseminates situation information and intelligence to management personnel. Planning Section prepares status reports, displays situation information, maintains the status of resources assigned to the measure's adoption and implementation, and prepares and documents the cyber risk mitigation measure implementation plan based on the Operations Section's input. A number of technical specialists may be appointed or otherwise engaged to assist in evaluating the situation, developing planning options, and forecasting requirements for additional resources. The Planning Section also addresses the mission and policy needs of each ESS or jurisdictional agency, as well as interaction between jurisdictions, functional agencies, and, if applicable, private organizations.
- **Logistics**-Logistics Section is responsible for all service support requirements needed to facilitate effective and efficient incident management, including ordering resources. This section also provides facilities, security, supplies, equipment maintenance, and communications and information technology support.
- **Finance/Administration**-Finance/Administration Section provides management with finance and other administrative support services. Some of the functions that fall within the scope of this section are recording personnel time, maintaining vendor contracts, administering compensation and claims, and conducting overall cost analyses.

The remainder of this section provides the cyber risk mitigation segments and measures and designates responsibility for their implementation, as recommended by the ESS Cyber Working Group. One important point to keep in mind is that the *Roadmap* articulates capability needs to reduce risks and is not a project or program planning document.

1. PRESERVING AND PROTECTING CITIZEN ACCESS TO EMERGENCY SERVICES

The ESS exists to serve the public during times of greatest need through its public safety disciplines; therefore, it is essential that public access to services is maintained. The cyber risk mitigation measures in this segment of the Roadmap address cyber risks identified in the ESS CRA that may affect that accessibility.

1.1. Adopt and Implement Next Generation 9-1-1 Services

The nationwide telephone number reserved for reporting emergencies in the U.S. is 9-1-1. This number was identified and established almost 50 years ago as a means of improving access to emergency services for the public, who often had no direct knowledge of the local telephone numbers for such agencies as sheriff's offices, police departments, fire departments, or rescue squads. The technology involved in providing 9-1-1 service for citizen-to-authority access (that is, the direct ability of the public to reach emergency services to request assistance) has evolved greatly. For example, advances in technology allow automated call switching and telephony, and fiber optics provide for more flexible and resilient connectivity between end users and carrier circuits and central offices. Furthermore, touch-tone service has been eclipsed by a variety of texting, data, and video communications capabilities that are available to the general public but cannot be used when calling 9-1-1 for help. This has changed with the advent of Next Generation 9-1-1 services.

1.1.1 Addressing Cyber Risks through Next Generation 9-1-1

Next Generation 9-1-1 is the next iteration of emergency communications services offered through a modernized architecture that supports the latest commercial communications offerings. Consumer-grade electronics development has outpaced the advancements of the legacy Basic and Enhanced 9-1-1 systems. Devices such as smartphones allow citizens to transmit not only voice calls, but text messages, pictures, video, and data as well. According to the United States Department of Transportation's (USDOT) National Highway Traffic Safety Administration (NHTSA), there is consensus among 9-1-1 stakeholders that the time has come to update the 9-1-1 infrastructure to enable the transmission of this type of digital information from callers to the emergency responder community via the 9-1-1 center. Next Generation 9-1-1 is a system of 9-1-1 services and databases that run on an Internet Protocol (IP)-based network that allows automatic and advanced sharing of digital data among all public safety responders, Public Safety Answering Points (PSAP), emergency management, traffic operations, and other entities. Next Generation 9-1-1 will allow for standards-based systems to provide reliability in the event of outages, scalability across all types of jurisdictions, and extensibility as new technology is developed. According to the National Emergency Number Association (NENA), Next Generation 9-1-1 uses IP-based systems comprised of managed Emergency Services IP networks (ESInets), functional elements (applications), and databases that replicate traditional Enhanced 9-1-1 features and functions and that provide additional capabilities. Next Generation 9-1-1 is designed to

provide access to emergency services from all connected communications sources other emergency service organizations.[2]

The ESS Cyber Working Group suggested that adopting Next Generation 9-1-1 would address a number of cyber risks associated with citizen access to emergency services. In the ESS CRA, one of the evaluated cyber risk scenarios is a natural disaster that causes the loss of 9-1-1 capabilities. This scenario would have compounding consequences. If any natural disaster is significant enough to render 9-1-1 communications inoperable, it would also likely damage property and may cause injury or loss of life to persons in the surrounding communities. The most catastrophic dimension of this scenario is the case where numerous citizens are in need of 9-1-1 for assistance but this capability is unavailable via traditional communications means, such as telephone. If a natural disaster causes the loss of 9-1-1 capabilities, the Public Safety Answering Point (PSAP) that receives and processes 9-1-1 calls for the proper deployment of ESS resources will be unable to perform an essential part of its mission. In turn, the operational capabilities across the ESS disciplines are put at risk. The consequences of the loss or degradation of 9-1-1 capabilities can cascade across several different critical infrastructure sectors and can significantly affect the ability of ESS to perform emergency response.

A denial of service due to an overloaded communications network is another ESS CRA cyber risk scenario that could limit access to 9-1-1 services. This scenario specifically focused on the loss of available public safety communications and public safety coordination/fusion networks from a denial of service. This scenario can occur deliberately from a malicious actor launching a denial-of-service attack, but it is far more likely to occur unintentionally from a network overload caused by a sudden and unexpected surge in public use. In the worst cases, typical ESS services would be unavailable to citizens until the issues were resolved. However, a compounding factor of this type of scenario is that such an overload is likely the result of a catastrophic event, creating a situation in which emergency services agencies cannot be reached when the most people need help and in which the system is unresponsive or slow to respond, thus causing potential loss of life and damage to property.

While these scenarios were seen as risks for which a Next Generation 9-1-1 system may offer the best mitigation, its modern provisions of infrastructure and access may help mitigate other cyber risks as well through the following features:

- Internet Protocol (IP) Technology-While an ESS agency implementing Next Generation 9-1-1 will likely use an exclusive Emergency Services Internet or ESInet rather than the public Internet, this may open the PSAP to new cyber risks to which it had not been exposed to when using older "1A2 keyset" technology. Networks, even private ones, require protection from cyber risk. Using IP technology does permit the use of modern protective measures against cyber risks, such as automated threat detection, system monitoring for intrusion, and malware and spyware defeats. IP-based technology permits the development of call re-routing to prevent or reduce overloading PSAP operators, to provide (a) redundancies that were not previously achieved easily and (b) greater speed in restoring access to emergency services when a PSAP is damaged or destroyed. It

[2] For more about the definition of and technology associated with Next Generation 9-1-1, visit NENA online at http://www.nena.org/?NG911_Baseline.

allows the establishment of a "virtual PSAP" by bringing a mobile unit into an affected community and establishing connection to the IP-based 9-1-1 infrastructure.

- **Fiber Optic Connectivity**-Regarding the benefits of fiber optics over copper for connectivity, fiber optics is more robust in terms of risks posed by natural disasters. Fiber optic lines are more flexible and resilient than hard copper wire line, and incorporating fiber optic lines reduces the incidence of theft because so little of the lines used for connectivity to the PSAP incorporate copper. Fiber optic lines provide the capacity needed to handle increased call volumes during surge periods and permit call load management through the routing of excess calls to alternate PSAP facility operators with whom any primary PSAP operator has a prior agreement.
- **Digital Data**-The ability to send messages from citizens to authorities using data communications reduces cyber threats of overloaded circuitry as less capacity is required to move data than is required to send voice traffic, still images, or video clips. This reduces the vulnerabilities that a PSAP may face when a surge in calls may otherwise result in busy signals or calls dropped.
- **Seamless Call Transfer Possibilities**-Unlike Basic or Enhanced 9-1-1 telephone systems, a Next Generation 9-1-1 system supports seamless transfer capabilities among facilities, along with citizen-to-authority communications improvements, such as the transfer of video clips or other images to enhance the 9-1-1 service to both citizens and ESS agencies.

There are challenges associated with the possibilities provided by Next Generation 9-1-1, as the connectivity required to bring this into every public safety communications center is not yet available. This, however, is changing. As access to better wired and wireless infrastructure and connectivity systems and services widens, so too will the ability to use data and video capabilities beyond simple voice access and telephony to communicate between citizen and authorities and from authorities to other authorities. Implementing Next Generation 9-1-1 creates opportunities for making mutual aid or automatic aid agreements viable alternatives for PSAP operators to improve services.

Through the ability to route excessive calls to an alternate PSAP for more rapid answering and call processing or to establish field offices in mobile command posts, office trailers, or any other temporary facility (the virtual PSAP), PSAP operators can also develop more cost-effective redundancies than a fixed facility or an Emergency Operations Center pressed into use as a PSAP may offer. This ability also offers greater response and recovery speed for a PSAP facility to restore citizen access to 9-1-1 if their primary site is lost or damaged to cyber threats or any other threat. Further discussion about alternate facilities begins on page 22.

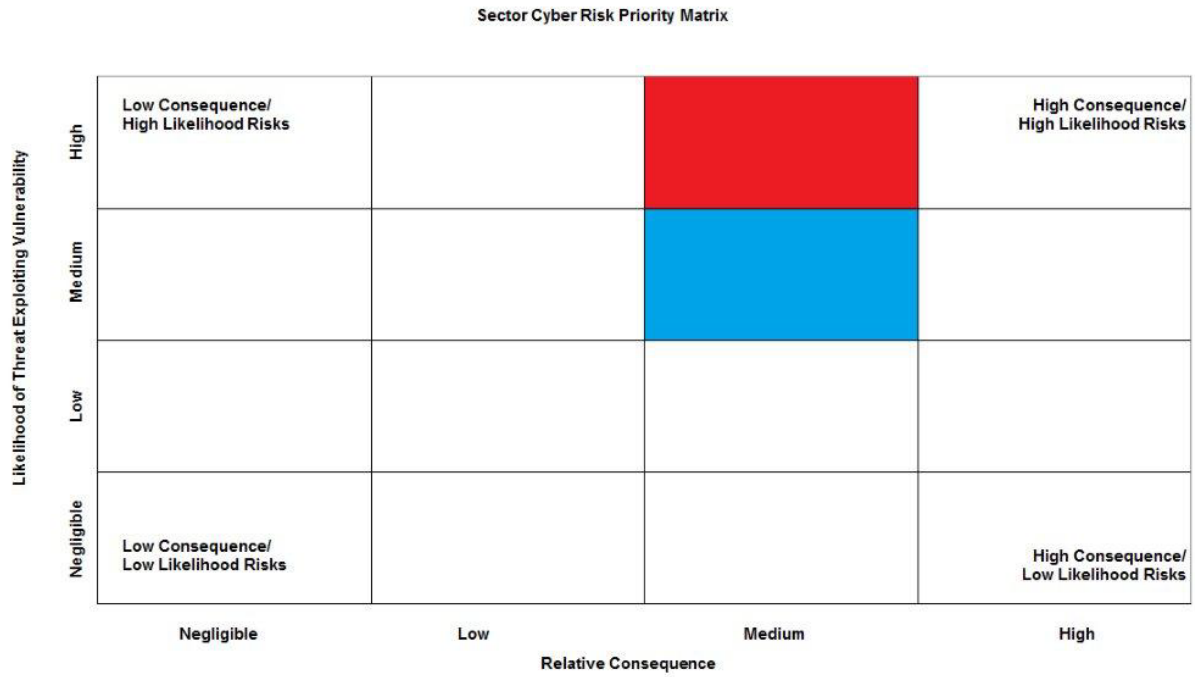
1.1.2 The Impact and Feasibility of Next Generation 9-1-1 as a Cyber Risk Reduction Measure

Implementation of Next Generation 9-1-1 specifically addresses the risks identified in but not limited to those in the ESS CRA natural disaster scenario. This technology would also address the risks associated with the threat of an overloaded PSAP or communications network, reducing what was evaluated as a very high-consequence cyber threat in the ESS CRA to a medium risk. A key constraint that any agency planning to adopt Next Generation 9-1-1 must address is the dependency on available and compatible infrastructure from commercial carriers to support this technology. It is essential that commercial carrier networks interface with the PSAP with any technology. At the time of the Roadmap

publication, the Federal Communications Commission (FCC) is working to adopt the rules that govern how commercial carriers will provide Next Generation 9-1-1, including specifications for the infrastructure required to serve any PSAP. In pursuing Next Generation 9-1-1 upgrades, commercial carriers must comply with the FCC requirements to implement the necessary technology that will permit ESS customers to acquire Next Generation 9-1-1 capabilities.[3]

Next Generation 9-1-1 systems provide a risk reduction from a high likelihood and consequence of being exploited by a cyber threat to a medium likelihood of cyber threat and a moderately high consequence if that threat were to be realized. This was identified in an analysis of the risk mitigation measures on 9-1-1 access during natural disasters, and this mitigation measure was also seen as an effective response to a PSAP encountering overloaded circuits or connectivity due to either natural or unintentional manmade incidents, such as a surge in demand for 9-1-1 services due to an emergency. Figure 2 below depicts the level of risk reduction that implementing a Next Generation 9-1-1 system would provide.

Figure 2. Estimated Level of Cyber Risk to 9-1-1 Telephone Systems, as Depicted by the Red Block. Cyber risk analysis indicates, via the blue block, the reduction of cyber risk that could be realized if a Next Generation 9-1-1 system were deployed as a mitigation measure against natural disasters. A Next Generation 9-1-1 system was also seen as an effective cyber risk mitigation measure against overloaded circuits and services, as these systems readily support rollover capabilities that can relieve an overloaded PSAP or its connectivity, another cyber risk scenario identified in the ESS CRA.



[3] There is an ongoing FCC proceeding dedicated to implementing Next Generation 911 service. The most recent decision is Facilitating Deployment of Text-to-911 and Other Next Generation 9-1-1 Applications, 78 Fed. Reg. 32169 (May 29, 2013).

Federal support in terms of policy, law, technical assistance, and (to a very limited extent) funding is available to enable PSAP operators to pursue the implementation of Next Generation 9-1-1 service to their constituents. The political risks of adopting Next Generation 9-1-1 are relatively low; the risks that do exist can be mitigated with appropriate planning and involvement of affected stakeholders. There are many citizens and organizations already using a number of consumer-grade devices to communicate with one another. Moving from citizen-to-citizen to citizen-to-authority capability brings PSAP operators into the age of modern communications. The goals and objectives of a Next Generation 9-1-1 system are consistent with the goals and objectives of having Basic or Enhanced 9-1-1 services now and increases the ability of call takers to field calls from citizens using voice, data, and video communications capabilities. It is likely that in some states existing policies and standards would mesh well with this new technology, although updates would be required in other states in which existing policies inhibit the adoption of Next Generation 9-1-1 standards.

Next Generation 9-1-1 systems do provide some other challenges for PSAP operators, however. The feasibility for operators to bring this new technology into existing public safety communications facilities and telephone company central offices will vary widely across the country. Much more coordination and collaboration will be required to implement Next Generation 9-1-1 than was necessary with legacy Basic or Enhanced 9-1-1 systems. In some locations, a new PSAP or call switching facility may be required; in others, an existing facility new PSAP or to develop alternate sites owned or operated by the PSAP agency to have a Cold or Warm Site[4] to provide backup capabilities may be significant. The culture among PSAP call taking staff may vary as well; for example, staff members who are prolific users of consumer-grade devices such as Smartphones, portable computing devices, and enhanced special mobile radio services may readily accept the changes that Next Generation 9-1-1 will bring. On the other hand, those staff members who do not use or who make limited use of wireless communications devices may find it more difficult to adapt to processing calls received from so many mediums. Finally, the time required to develop plans, to identify funding, and to partner with all appropriate entities to acquire and implement Next Generation 9-1-1 services means that neither this nor the development and approval process for rollover agreements is not a short-term solution or cyber risk mitigation measure. This mitigation measure will likely take greater than 24 months to implement.

1.1.3 Organizational Responsibilities for Implementing Next Generation 9-1-1

The issue of responsibility for acquiring Next Generation 9-1-1 in a given community can be complex. First, there must be public support for the acquisition. This may be expressed in the form of hearings to discuss the possibilities, benefits, and impacts of bringing Next

[4] Cold Sites and Warm Sites, along with the term 'Hot Site,' are business continuity planning terms for backup facilities to quickly discern their readiness. A Cold Site, for example, is a defined facility that may have varying levels of capabilities installed. A Cold Site may have connections and power from the outside into the facility, but it may have no installed equipment ready to be activated to serve as a PSAP. It is not staffed, and the time required to activate the site may range from hours to weeks, depending upon the level of desired readiness. A Warm Site, on the other hand, is a defined facility with those connections and with the backup equipment installed. It is ready to be staffed and to be activated, but systems may take some time to activate. Generally, a Warm Site requires minutes to hours to accomplish this. A Hot Site may also be available; these are sites that are defined, equipped, staffed, and ready to activate on short or no-notice. There are not many Federal, State, local, tribal, or territorial PSAP operators who can afford the costs and complexities of operating Hot Sites.

Generation 9-1-1 to the community. This may be in the form of voter support for bond referenda or other funding mechanisms sought to finance the acquisition. It may come from elected government officials who review and approve budgetary appropriations for the costs to acquire and implement a Next Generation 9-1-1 system, or it may be a combination of these indicators.

The key authority or group overseeing the implementation of a Next Generation 9-1-1 system will vary depending upon the level of government involved. This could be a state's 9-1-1 or PSAP coordinator, or it could be initiated by a number of local-level officials, such as a 9-1-1 or PSAP oversight body, a city manager, a county's chief information officer. Table 2 on the next page depicts how such a key authority or group could delegate responsibilities for developing, acquiring, and implementing a Next Generation 9-1-1 system, coupled with efforts to design and execute failover exercises and to develop rollover capabilities.

Table 2. Cyber Risk Mitigation using Next Generation 9-1-1.

Implementing a Next Generation 9-1-1 System for Cyber Risk Mitigation
Key authority or group:
Varies by jurisdiction; state 9-1-1 or PSAP Coordinator, city manager, county CIO, regional 9-1-1 or PSAP authority are all possibilities. • Assess public support and the political will to acquire a Next Generation 9-1-1 system • Identify funding sources to finance acquisition and operation
Primary Organizational Responsibility:
9-1-1/PSAP services planning body; at the local or State level, this may be the State 9-1-1 or PSAP coordinator, a 9-1-1 or PSAP service authority, or other organization. • Involve State 9-1-1 coordinators in any methods of implementation or measurement of implementation. • Reach to Federal resources for guidance. The National 9-1-1 Program at USDOT/NHTSA is a likely source for planning support. • Research the work of the Federal Communications Commission (FCC), which has been working with telecommunications service providers and local exchange carriers on resilience of telephone networks in the face of natural disasters. For example, the FCC has done work with Verizon® and AT&T® related to major power outages during derecho storms, and lessons learned therein may be useful. • Close coordination with the local exchange carriers will be needed to ensure that the telephone networks are developed to support Next Generation 9-1-1 services even as the actual system acquisition for the PSAP is being planned.
Secondary Organizational Responsibilities:
Operating PSAP facilities • Develop policies, practices, and procedures that will support acquisition and implementation of Next Generation 9-1-1 and develop the training necessary to ensure that it is properly operated.
Finance/administrative aspects of the PSAP • Ensure that legal and policy support and fiscal resources are available and can be authorized to engage in such exercises and agreements.
Logistical support • Procure the necessary equipment and furnishings based on operational requirements and the approval of the administrative/finance organization. • Provide any logistics needed to support activation of rollover agreements or to conduct training and exercises on failover procedures.

As indicated in Table 2, there is heavy Federal engagement and influence in developing Next Generation 9-1-1 systems in the U.S. The USDOT/NHTSA has engaged in a campaign to bring multiple modes of communications into the ESS for citizen-to-authority contact and has developed the architecture to encourage greater development in the sector through test bed trials. NHTSA has also created a National 9-1-1 Program[5] to provide access to Federal resources and technical expertise and has procured grant funding to help PSAP operators take the next steps and move from seven-ten digit emergency lines, Basic 9-1-1, or Enhanced 9-1-1 to Next Generation 9-1-1.

[5] More information about the USDOT/NHTSA initiative is available online at http://911.gov.

1.2 Create and Implement an Alternative Emergency Number to 9-1-1 and/or Expand the Number of Available 9-1-1 Trunk Lines

Historically, before the creation of n-1-1 telephone numbers for any interactions with organizations beyond telephone service providers, ESS agencies used 7- or 10-digit telephone numbers for citizen-to-authority calls requesting help. When 9-1-1 was established as the National Emergency Telephone Number across the country, many agencies began adopting this technology to provide access to the communities they serve. Nonetheless, many agencies continue to use those 7- or 10-digit telephone numbers to receive emergency telephone calls. Creating and implementing an alternative emergency number to 9-1-1 and/or expanding the number of available 9-1-1 trunk lines as a cyber risk mitigation measure focuses on 9-1-1 system operators; however, those agencies still using 7- or 10-digit telephone lines may also benefit from this measure.

The ESS CRA acknowledged that a limited number of trunk telephone lines at PSAP facilities exist to receive emergency calls and considered a scenario in which callers may receive a busy signal when dialing 9-1-1. Overloaded communications networks can occur as a result of a malicious actor launching a denial of service attack or as a result of an unintentional network overload caused by a sudden and unexpected surge in public use. Implementation of an alternative emergency number to 9-1-1 and/or expansion of the current trunk lines will enable public safety call takers and dispatchers to continue their duties in the event of an incident that disables or jams the primary lines for 9-1-1 caller communications.

1.2.1 Addressing Cyber Risks through Alternative Emergency Numbers and/or the Expansion of Available 9-1-1 Trunk Lines

The ESS Cyber Working Group determined that establishing an alternative emergency number to 9-1-1 and/or expanding the number of available 9-1-1 trunk lines will slightly reduce the extent of vulnerability exposure but will significantly reduce the consequence of an event from high to low, particularly regarding economic security and public confidence in the affected area. In the ESS CRA, one of the scenarios evaluated manmade deliberate and unintentional threats that could result in the loss or degradation of 9-1-1 and other emergency mobile communications. Loss of communications could also result in the inability to deploy resources, the loss of public confidence in emergency services, and confusion or panic. In worst case scenarios, ESS access could be unavailable to citizens until normal capabilities became available again; an alternative emergency number or an expansion of trunk lines could provide partially-to-no uninterrupted access during this loss of communication network service.

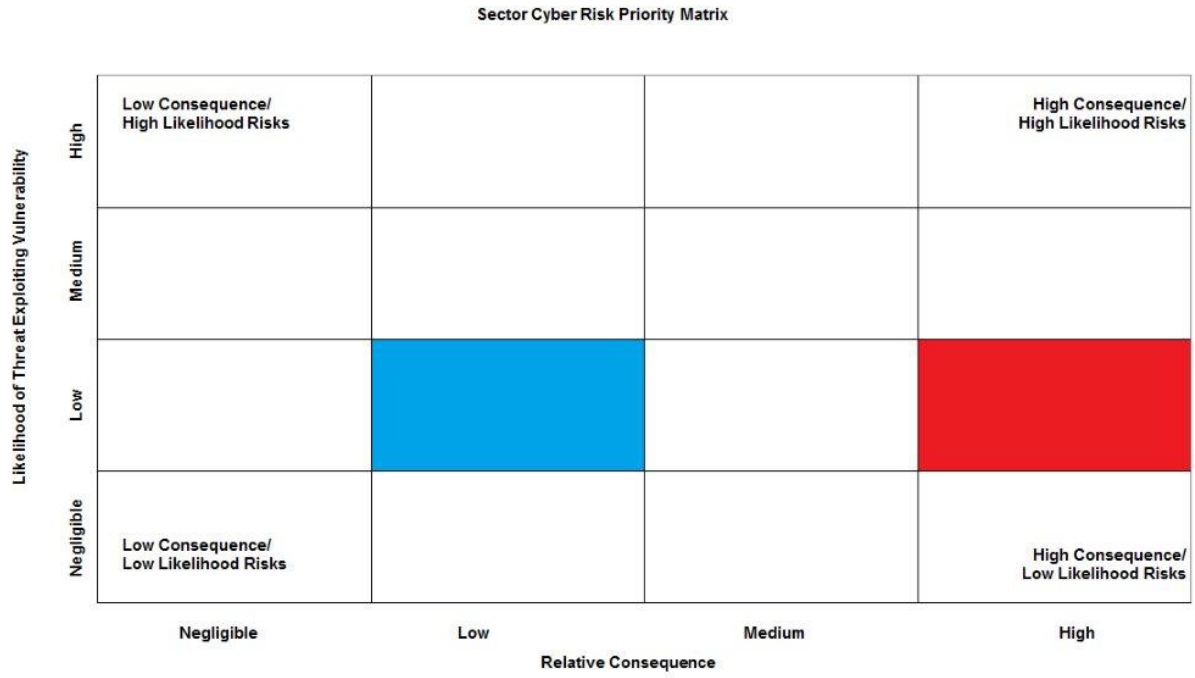
1.2.2 The Impact and Feasibility of Alternative Emergency Numbers and the Expansion of Available 9-1-1 Trunk Lines as Cyber Risk Reduction Measures

Implementation of alternative emergency numbers and the expansion of available trunk lines address risks identified in the specific ESS CRA scenario. As many agencies have retained legacy 7- or 10-digit emergency telephone numbers, alternate emergency numbers already exist. For those agencies that have discarded those legacy emergency telephone numbers, existing non- emergency telephone numbers may provide the ability to redirect public emergency calls when combined with a public alert to notify them of the degradation

of 9-1-1. In a crisis, it is likely that the people in a jurisdiction served by a PSAP will use information and methods with which they are already familiar to reach emergency services. Nonetheless, alternatives should be planned, whether it is using an existing 7-10 digit emergency number, using an existing non-emergency number, alerting the public to report to neighborhood police or fire stations for emergency services, or, for agencies with staff members trained and equipped, offering alternatives related to social media or text messaging to reach an agency when help is needed.

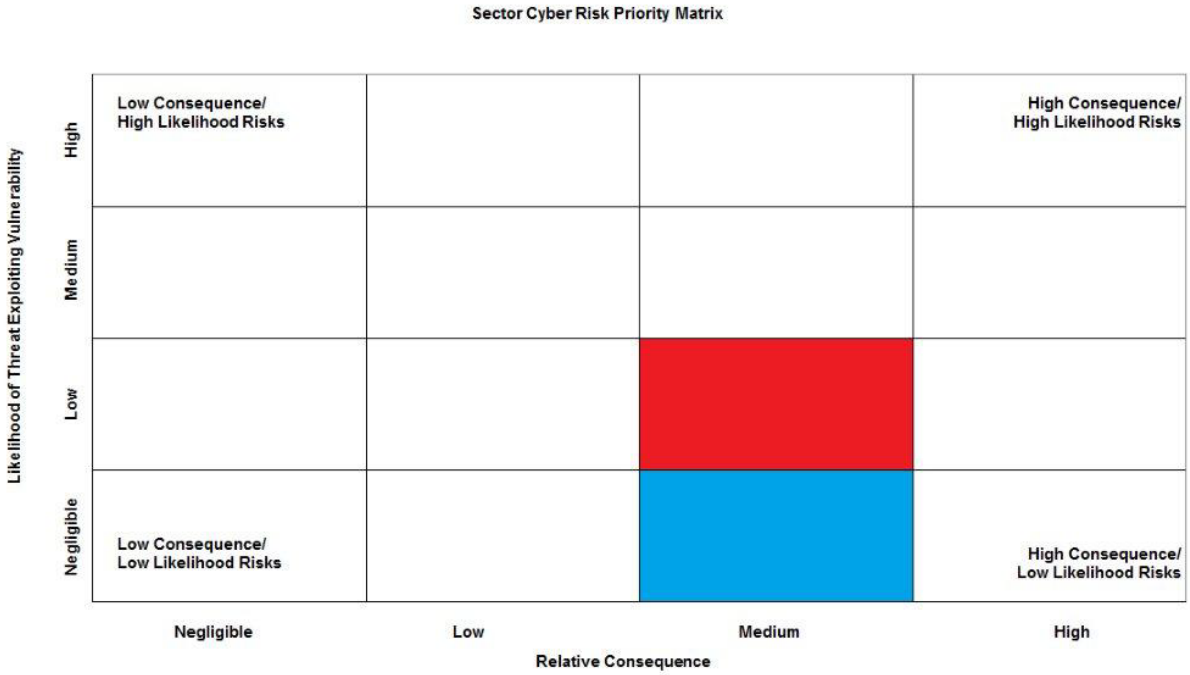
Regarding a deliberate manmade threat, the establishment of an alternative emergency number to 9-1-1 and/or expanding the number of available 9-1-1 trunk lines will slightly reduce the extent of vulnerability exposure but will significantly reduce the consequence of an event to low (as shown in Figure 3 below), particularly regarding adverse financial costs associated with the effected region's loss of communications and public confidence.

Figure 3. Estimated Level of Cyber Risk to Overloaded Communications Network, as Depicted by the Red Block. Cyber risk analysis indicates, via the blue block, that the reduction of cyber risk that could be realized if alternative emergency numbers and/or the expansion of available 9-1-1 trunk lines were implemented as a mitigation measure against deliberate manmade threats.



Pertaining to unintentional manmade- threats, establishing an alternative emergency number to 9-1-1 and/or expanding the number of available 9-1-1 trunk lines will slightly reduce vulnerabilities but will have no effect on consequence (as shown in Figure 4 on the following page).

Figure 4. Estimated Level of Cyber Risk to Overloaded Communications Network, as Depicted by the Red Block. Cyber risk analysis indicates, via the blue block, that the reduction of cyber risk that could be realized if alternative emergency numbers and/or the expansion of 9-1-1 trunk lines were implemented as a mitigation measure against manmade-unintentional threats.



1.2.3 Organizational Responsibilities for Implementing Alternative Emergency Numbers and Expanding Available 9-1-1 Trunk Lines

A key group of authorities, such as 9-1-1 coordinators, relevant chief information officers, and local exchange carriers will play an important role in pursuing this cyber risk mitigation measure. They can identify the public and political resources needed to approve the implementation and determine potential sources needed to acquire financial support. These key authorities should also assess if the actual physical facility can support additional staff to receive and process calls. Additional costs (e.g., acquisition, personnel, maintenance) may occur when using additional 9-1-1 trunk lines or alternate emergency telephone numbers. Key authorities identify whether the possibility that an alternative number to 9-1-1 (such as a legacy 7–10 digit emergency telephone line) already exists and whether the public is aware of its existence. Organizations operating PSAP facilities should work to create the policies and procedures needed to help decide when to use the alternative number and how to announce it to the public and media.

Additional actions that should be taken to support implementing alternative emergency numbers and expanding available 9-1-1 trunk lines can be found in Table 3 on the following page.

Table 3. Cyber Risk Mitigation Using Alternative Emergency Numbers and/or Expanding Available 9-1-1 Trunk Lines.

Implementing Alternative Emergency Numbers and/or Expanding Trunk Lines for Cyber Risk Mitigation
Key authority or group:
Varies by jurisdiction; State 9-1-1 or PSAP Coordinator, city manager, county CIO, regional 9-1-1 or PSAP authority are all possibilities. • Assess public support and the political will to acquire a Next Generation 9-1-1 system • Identify funding sources to finance acquisition and operation
Primary Organizational Responsibility:
9-1-1/PSAP services planning body; at the local or State level, this may be the State 9-1-1 or PSAP coordinator, a 9-1-1 or PSAP service authority, or other organization. • Involve state 9-1-1 coordinators in any methods or measurement of implementation. • Reach to Federal resources for guidance. The National 9-1-1 Program at USDOT/NHTSA is a likely source for planning support. • Research the work of the Federal Communications Commission (FCC), which has been working with telecommunications service providers and local exchange carriers on resilience of telephone networks in the face of natural disasters. For example, the FCC has worked with Verizon® and AT&T® related to major power outages during derecho storms, and lessons learned therein may be useful. • Work with local exchange carriers to determine if sufficient trunk lines are available to reach an alternative number.
Secondary Organizational Responsibilities:
Operating PSAP facilities • Develop policies, practices, and procedures that will support alternative number or additional trunk line implementation and establish the training necessary to ensure that they are properly operated. • Develop training and exercises needed to become proficient in executing mitigation procedures, including the activation of alternate PSAP facilities and the activation/deactivation of rollover agreements if additional facilities are needed.
Finance/administrative aspects of the PSAP • Ensure that legal and policy support and fiscal resources are available and can be authorized to engage in such exercises and agreements.
Logistical support • Procure necessary equipment and furnishings based on operational requirements and the administrative/finance organization's prior approval. • Provide logistics needed to support the activation of agreements or to conduct training and exercises on failover procedures.

As indicated in Table 3, there is low Federal engagement and influence involved in implementing alternative emergency numbers and expanding the number of trunk lines. Specific requirements and constraints will vary by jurisdiction, but most of the progress and constraints will concentrate at the local and state levels.

2 PROTECTING FACILITY AND CYBER INFRASTRUCTURE CAPABILITIES

ESS agencies rely on key facilities and their supporting cyber infrastructure to deliver services to the public. This segment of the *Roadmap* covers cyber risk mitigation measures that protect facility and associated cyber infrastructure capabilities.

2.1 Create Alternate Emergency Operation Centers and Additional Public Safety Answering Point Facilities

The ESS Cyber Working Group recommends addressing the potential loss of 9-1-1 capabilities, which can be accomplished by creating alternate Emergency Operations Centers (EOC) and additional PSAP facilities as a proactive mitigation measure.

2.1.1 Addressing Cyber Risks through Alternate Emergency Operation Centers and Public Safety Answering Point Facilities

Establishing alternate EOC Emergency Operations Centers (EOC) and PSAP facilities can minimize the risk of a disabled emergency communications center due to a natural disaster or other debilitating scenario. In the ESS CRA, one of the scenarios considered a cyber risk is a natural disaster causing the loss of 9-1-1 capabilities. In this case, the operational capabilities across the ESS disciplines—including the law enforcement, fire and emergency services, public safety communications, public works, and emergency medical services—are put at risk. Consequences could include the loss of or damage to the emergency communications center as well, which can disrupt emergency communications across several different critical infrastructure sectors and can significantly affect the ability of ESS to perform emergency response. Alternate EOC and/or PSAP facilities provide a redundant source for emergency communications operations in the event that the primary or active facility becomes inoperable. Additionally, implementing Next Generation 9-1-1—another proposed mitigation strategy for the natural disaster scenario—and establishing alternate facilities ensures a smooth transfer from the affected facility to the reserve facility, reducing downtime for 9-1-1 services.

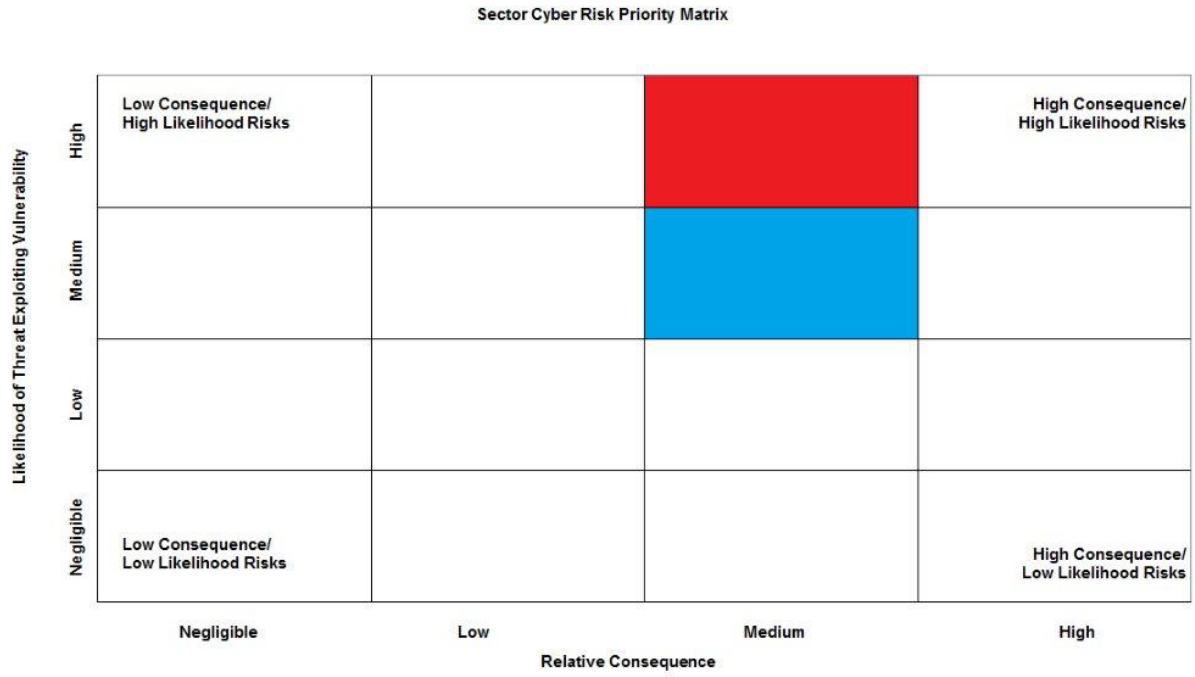
The ability to route calls to an alternate PSAP for more rapid answering and call processing or to establish field offices in mobile command posts, office trailers, or any other temporary facility (the virtual PSAP) means that PSAP operators can also develop more cost-effective redundancies than a fixed facility or an EOC pressed into use as a PSAP may offer. That ability also offers greater response and recovery speed for a PSAP facility to restore citizen access to 9-1-1 if their primary site is lost or damaged due to cyber threats or other threats.

2.1.2 The Impact and Feasibility of Alternate Facilities as a Cyber Risk Reduction Measure

Alternate EOC and PSAP facilities specifically address the risks identified from the natural disaster scenario of the ESS CRA also in addition to addressing risks associated with the threat of an overloaded PSAP or communications network. Establishing automatic or mutual aid agreements in advance and developing rollover capabilities to re-route calls to an alternate PSAP provides a risk reduction from high likelihood and consequence to a medium likelihood of cyber threat and a moderately high consequence. Thus, establishing rollover capabilities is a significant cyber risk mitigation measure. PSAP development would be done in accordance with all applicable international, Federal, state, local, tribal and territorial

treaties, laws, and policies. Figure 5 below depicts the level of risk reduction that implementing alternate EOC or PSAP facilities would provide.

Figure 5. Estimated Level of Cyber Risk to 9-1-1 Telephone Systems, as Depicted by the Red Block. Cyber risk analysis indicates, via the blue block, that the reduction of cyber risk that could be realized if an alternate EOC and/or PSAP facility were established and activated as a mitigation measure against natural disasters.



Challenges exist for this mitigation response, however, and its feasibility has not yet been fully vetted. Constraints affecting feasibility include financial requirements for implementation, time to implement, and potential difficulties with system compatibility. If an alternate PSAP does not already exist, the costs for a new PSAP or to develop alternate sites owned or operated by the PSAP agency to have a Cold or Warm Site to provide backup capabilities may be significant. Existing organizational practices resistant to implementation, technological viability, and the Emergency Services Sector's cultural environment may also present moderate constraints to implementation.

The plan for implementation will vary by agency, geographical location, and existing resources. If prone to natural disasters, a jurisdiction should consider other locations to host its alternate facility. As a result, this mitigation measure may require agreements with neighboring counties, towns, and states, as well as with jurisdictions outside the scope of a disaster area. For example, intergovernmental agreements (automatic or mutual aid) are widely used and available, but those that need to support rollover capabilities have not been executed to any great extent to date. The legal and political support for such agreements exists, but some thought as to the mechanisms to activate these agreements to address issues of duration of rollover operations, responsibility for associated costs (for personnel surge, technology switches, and information management and dissemination, as examples), and compatibility between PSAP facilities would be required before these agreements could be developed and signed. However, if implemented successfully, these agreements and the

alternate facilities they provide could increase redundancy and reduce consequences from large-scale disasters affecting both primary and back-up facilities.

The plan for implementation will also differ between establishing an alternate EOC versus an alternate PSAP. While a PSAP provides operational and technological capabilities, an EOC allows the gathering of policy and decision makers to focus on planning and collaboration. In many primary locations, a PSAP and an EOC are co-located within the same facility. When not co-located, activating an alternate EOC may be simpler than activating an alternate PSAP because an alternate EOC does not require a PSAP's equipment and technology, such as dispatch phones and radios. An alternate PSAP with its technological requirements would be more vulnerable to a cyber risk and would experience more significant consequences in its ability to perform its mission. This mitigation measure will likely take greater than 24 months to implement because of the equipment required for activation, staffing decisions and resources, and the process of determining whether the alternate facility should be a Hot, Cold, or Warm site.

2.1.3 Organizational Responsibilities for Implementing Alternate Emergency Operation Centers and Public Safety Answering Point Facilities

The issue of responsibility for activating an alternate EOC or PSAP facility in a given community can be complex. The key authority or group overseeing the implementation of alternate sites will vary depending upon the level of government involved. This could be a state's 9-1-1 or PSAP coordinator, or it could be initiated by a number of local level officials, such as a 9-1-1 oversight body, a city manager, a county's chief information officer, or any other designated official or body with oversight responsibilities for acquiring and delivering citizen access to 9-1-1. Table 4 on the following page depicts how such a key authority or group could delegate responsibilities for establishing an alternate EOC or PSAP facility, coupled with efforts to design and execute failover exercises and to implement Next Generation 9-1-1.

Table 4. Cyber Risk Mitigation Using Alternate EOC and PSAP Facilities.

Creating an Alternate EOC or PSAP Facility for Cyber Risk Mitigation
Key authority or group:
Varies by jurisdiction; state 9-1-1 or PSAP Coordinator, city manager, county CIO, regional 9-1-1 or PSAP authority are all possibilities. • Assess public support and the political will to acquire a Next Generation 9-1-1 system • Identify funding sources to finance acquisition and operation
Primary Organizational Responsibility:
9-1-1/PSAP services planning body; at the local or state level, this may be the state 9-1-1 or PSAP coordinator, a 9-1-1 or PSAP service authority, or other organization. • Involve state 9-1-1 coordinators in any methods or measurement of implementation. • Research the work of the FCC, which has been working with telecommunications service providers and local exchange carriers on the resilience of telephone networks in the face of natural disasters. For example, the FCC has worked with Verizon® and AT&T® related to major power outages during derecho storms, and lessons learned therein may be useful. • Close coordination with the local exchange carriers will be needed to ensure that the telephone networks services can be switched to the alternate facility even as the actual system acquisition for the alternate EOC or PSAP is being planned.
Secondary Organizational Responsibilities:
Operating PSAP facilities • Develop policies, practices, and procedures that will support alternate facility activation, and initiate training necessary to ensure that it is properly operated. • Develop training and exercises needed to develop proficiency in executing failover procedures, including activation of alternate PSAP facilities and activation/deactivation of rollover agreements.
Finance/administrative aspects of the PSAP • Ensure that legal and policy support and fiscal resources are available and can be authorized to engage in such exercises and agreements.
Logistical support • Procure necessary equipment and furnishings based on operational requirements and the administrative/finance organization's prior approval. • Provide logistics needed to support the activation of rollover agreements or to conduct training and exercises on failover procedures.

As indicated in Table 4, low Federal engagement and influence are required to activate alternate PSAP or EOC facilities. Specific requirements and constraints will vary by jurisdiction, but most of the progress and constraints will concentrate at the local levels.

2.2 Create Diversity in Public Safety Answering Point and Communications Infrastructure Facilities

A PSAP is a facility at which 9-1-1 telephone calls are received and processed for dispatch. There are still ESS organizations that maintain other emergency communications call centers, such as secondary PSAP facilities (in which 9-1-1 calls are received elsewhere but are transferred to that facility if their particular agency is needed) and facilities that receive and process calls placed to an agency's 7- or 10-digit telephone number. These are examples of critical communication infrastructure facilities, but this cyber risk mitigation measure also covers other facilities, such as radio transmitter, receiver, and repeater tower

sites; equipment and radio repair centers; telephone switch centers; and central offices that serve PSAP and other emergency communications centers. While these latter three types of facilities may be owned, operated, or otherwise maintained by a commercial service, the ESS has a vested interest in promoting diversity in those facilities as customers demand the most reliable services available.

ESS agencies understand that communications infrastructure facilities provide the connectivity needed to provide citizen-to-authority communications and authority-to-authority communications. These connections support the delivery of the right type of service at the right location and at the right time, whether the need is for an urgent response from a single agency or for a coordinated response by two or more agencies. While the loss of that connectivity is most likely to occur due to unintentional manmade causes (such as the accidental severing of critical trunk lines due to a construction project some distance away), diversifying communications facilities can address a number of other cyber risks, such as natural disasters, as well.

2.2.1 Addressing Cyber Risks through Diversity in Public Safety Answering Point and Communications Infrastructure Facilities

As noted in the section on Next Generation 9-1-1, there can be challenges to creating diversity in a PSAP or other communications infrastructure facility. Nonetheless, it is important to understand the types of diversity that can serve as a cyber risk mitigation measures.

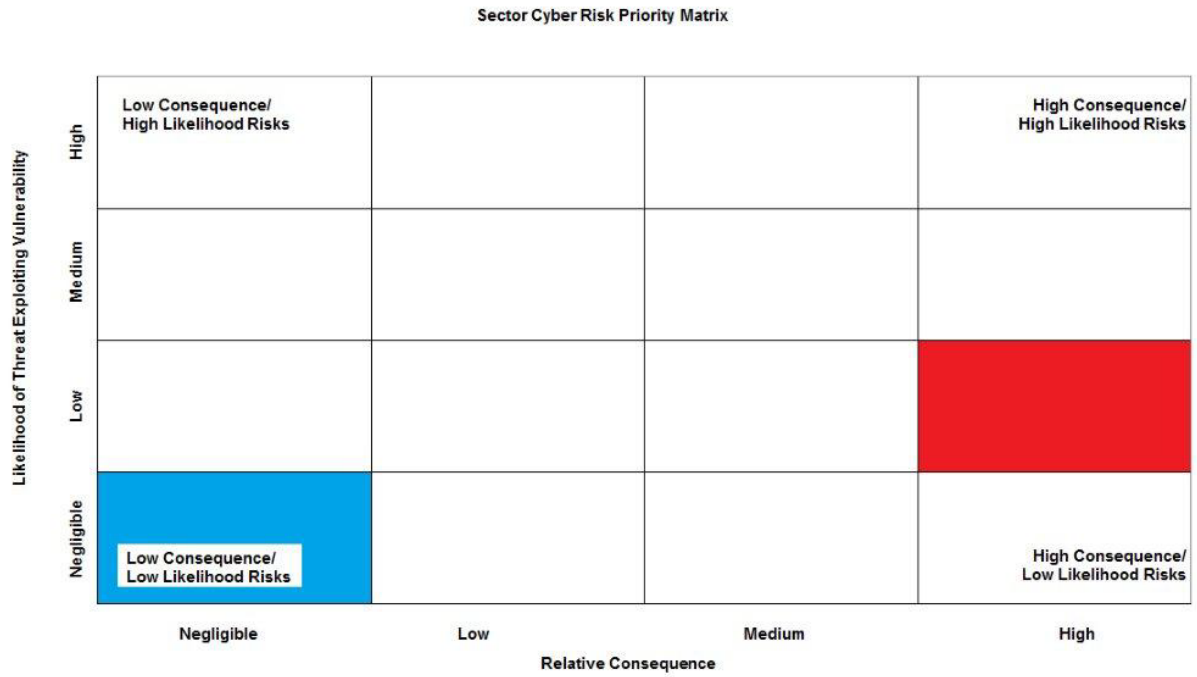
- Route Diversity-A significant exposure to cyber risk is the connectivity that links PSAP, communications facilities, supporting infrastructure (such as power sources), and end users. Route diversity refers to the establishment of more than one path to connect a PSAP or communications infrastructure facility with other sorts of facilities. For example, a telephone trunk that runs from a local exchange carrier's central office to a PSAP to carry Basic or Enhanced 9-1-1 calls placed in that central office's service area can run for miles and could be located either above grade (strung overhead between utility poles) or below grade (buried). If that single trunk line is severed when an auto strikes and breaks a utility pole on which that trunk line is carried, a significant number of citizens, businesses, or other ESS agencies could lose their ability to reach that PSAP. Route diversity could be accomplished by connecting that PSAP to an alternate central office, through which 9-1-1 calls could be routed or by bringing trunk lines into a PSAP from more than single direction. In the Next Generation 9-1-1 environment, in most instances instead of using dedicated trunks, selective routers, and number and location databases, these systems will use IP-based hardware and software to provide to provide call identification, location determination, call routing, and call signaling for emergency calls. Access to the ESInet will be made via IP gateways.
- Facility Diversity-A PSAP or other communications infrastructure site could have backup sites identified or developed. As noted in the discussion about Next Generation 9-1-1, backup sites provide an opportunity to ensure that calls can continue to be received and processed even if the primary PSAP is inaccessible. The same principle applies to other infrastructure sites, where overlapping coverage or provisioning of services ensures minimal or no disruption of services in the event that primary infrastructure sites are disabled, disrupted, or destroyed. This diversity could be achieved by pre-arranging rollover capabilities (as noted in the Next Generation 9-1-1 discussion) or transitioning to

a Continuity of Operations (COOP) site (as discussed in the cybersecurity and COOP plan implementation section, starting on page 43).

2.2.2 The Impact and Feasibility of Diversity in Public Safety Answering Point and Communications Infrastructure Facilities as a Cyber Risk Reduction Measure

An evaluation of this risk mitigation measure revealed that creating diversity in PSAP and communications infrastructure would significantly reduce the overall risk that a loss of communications lines would pose to the sector. Introducing diversity into PSAP facilities and establishing redundant radio network facilities or repeater sites will have a significant reduction in consequences, lowering it to an almost negligible level. This reduction is most significant in response to intentional acts that affect a PSAP or communications infrastructure facility, and it also reduces consequences for natural or unintentional disruptions. Assuming the basic infrastructure exists to support the required functions, it is estimated that this cyber risk mitigation measure could be developed in less than 24 months. That estimation could be higher depending upon the availability of route diversity and facilities to use for creating diversity in communications infrastructure. Figure 6 below depicts the risk reduction.

Figure 6. Estimated Level of Cyber Risk to PSAP or Other Communications Infrastructure Facilities, as Depicted by the Red Block.
Cyber risk analysis indicates, via the blue block, that the reduction of cyber risk that could be realized if diversity in PSAP and communications infrastructure facilities were used as a mitigation measure against natural disasters or unintentional manmade acts.



Creating diversity in PSAP and communications infrastructure facilities is a feasible response to cyber risk. Laws, rules, and regulations affecting the development and

implementation of diversity measures exist and are easily adopted. There is already a standard in the ESS for creating COOP sites and for fostering backup measures to ensure redundancy in critical systems, so it is likely that ESS staff and leaders would accept and support such efforts. The technology needed to implement this risk mitigation measure is readily available.

There are some concerns that may limit an agency's ability to adopt this cyber risk mitigation measure, however. The political will to establish diverse facility sites may be inhibited by a desire to invest within the confines of the political jurisdiction served by the PSAP or communications infrastructure facility. While this is understandable from the standpoint of community accountability, locating such facilities away from the threatened area may in fact be a better investment, even if those sites are beyond jurisdictional lines. . The fiscal resources needed to establish route diversity may be constrained due to the costs of paying for route diversity on an ongoing basis; such costs are not one-time only incursions. As with COOP sites, costs for developing alternate infrastructure sites can be higher than can be easily justified, and so careful consideration must be given to adding value to such sites. Offsetting costs for redundant radio tower sites by renting space out or sharing maintenance and operating costs with other communication system operators—commercial or governmental—can make such measures more cost effective.

2.2.3 Organizational Responsibilities for Creating Diversity in Public Safety Answering Point and Communications Infrastructure Facilities

The organizational responsibility for implementing this cyber risk reduction measure most likely lies with the key authority or group that provides emergency communications services (such as operating a PSAP or managing a land mobile radio system) for an ESS agency. At the Federal or state levels of government, this could be the telecommunications managers (such as wireless management offices) for a given department or agency and/or the state's 9-1-1 or PSAP Coordinator. As noted on page 46, Federal agencies must develop COOP plans per Presidential Decision Directive #8 – National Preparedness (PPD-8), and this risk mitigation measure supports compliance with that mandate. At the local or tribal levels of government, the responsible key authority may be the chief of a public safety agency, a radio system manager, or an information technology manager.

Table 5 on the following page depicts how such a key authority or group could delegate responsibilities for creating diversity in PSAP and communications infrastructure facilities.

Table 5. Creating Diversity in PSAP and Communications Infrastructure Facilities.

Creating Diversity in PSAP and Communications Infrastructure Facilities
Key authority or group:
Varies by jurisdiction; Federal or state telecommunications manager, the state 9-1-1 or PSAP Coordinator, local or tribal communications service provider, information technology manager, or radio system manager • Assess sufficiency and availability of COOP plans, backup sites, and route diversity available from local exchange carriers. • Identify funding sources to finance the development of diversity for affected communications facilities.
Primary Organizational Responsibility:
Varies by jurisdiction; Federal or state telecommunications manager, the state 9-1-1 or PSAP Coordinator, local or tribal communications service provider, information technology manager, or radio system manager that operates and maintains the PSAP and communications infrastructure facilities • Collaborate with local exchange carriers serving the affected infrastructure sites to discern the cost and availability of route diversity. • Develop requirements for diversity in communications infrastructure sites; these will be variable based on whether a PSAP is operated by the key authority or if other communications centers and supporting communications infrastructure, such as land mobile radio networks, must be supported. • Identify COOP sites or other infrastructure sites that could be used to establish facility diversity for tower sites and other communications infrastructure. • Assess the suitability of identified sites for development as a diverse facility for communications system support.
Secondary Organizational Responsibilities:
Operating PSAP facilities • Develop policies, practices, and procedures that will support alternate facility activation, and initiate training necessary to ensure that it is properly operated. • Develop training and exercises needed to develop proficiency in executing failover procedures, including activation of alternate PSAP facilities and activation/deactivation of rollover agreements.
Finance/administrative aspects of the PSAP • Ensure that legal and policy support and fiscal resources are available and can be authorized to engage in the development of route and facility diversity measures.
Logistical support • Procure necessary equipment and furnishings based on operational requirements and the administrative/finance organization's prior approval. • Provide logistics needed to support the activation of rollover agreements or to conduct training and exercises on failover procedures.

As indicated in this table, there is little Federal engagement or influence in creating diversity in PSAP and communications infrastructure facilities. This is largely an agency-specific risk mitigation measure. The Next Generation 9-1-1 programs described starting on page 11 will be of use to PSAP operators.

2.3 Implement Improved Physical Security Measures at Public Safety Answering Point and Communications Infrastructure Facilities

PSAP facilities and other emergency communications centers (referred to in general as PSAP facilities in this section) function as the main hub for all incoming emergency services

requests. Emergency call takers and dispatchers conduct their daily operations out of these facilities. When a 9-1-1 or other emergency number is dialed to request emergency services, call takers answer the call and record the necessary information to ensure that proper resources can be dispatched. Dispatchers send the most appropriate available public safety resources to render aid. For these PSAP facilities and related communications infrastructure to function, the use of specific equipment is required, such as telephone sets, land mobile radios, computer-aided dispatch systems, along with supporting infrastructure components such as transmission and repeater sites, radio towers, and telephone central offices. As such, physical security is a cyber risk mitigation measure that should be implemented and used not just at PSAP or other emergency communications centers and facilities but across all communications infrastructure sites that support an ESS agency's emergency communications capabilities. This includes those remote sites that host those additional components.

Currently, there are both Basic 9-1-1 and Enhanced 9-1-1 systems in use around the country, in addition to traditional 7- and 10-digit emergency telephone numbers. However a newer system, Next Generation 9-1-1, is in early stages of implementation. This system promises enhancements that could make both Basic and Enhanced 9-1-1 systems obsolete. The Basic and Enhanced 9-1-1 systems use copper wire to provide connectivity between telephone company central offices and PSAP facilities and to land mobile radio infrastructure sites. As technology advances and costs to acquire and deploy copper wire increase, this material is being replaced by fiber optic lines for its resilience, its ability to support greater communications capacity, and its availability at acceptable costs. Copper is also highly desired by criminals, as it has a high street value as scrap metal. Physical security measures to protect the connectivity essential to the smooth and uninterrupted flow of PSAP and other emergency communications is essential in keeping access to emergency services resources available to the public.

2.3.1 Addressing Cyber Risks through Improved Public Safety Answering Point Physical Security Measures

The ESS Cyber Working Group suggests that implementing improved physical security measures to PSAP facilities and their supporting infrastructure would address a number of cyber-related risks that could damage the public's ability to gain access to emergency services. The related *ESS CRA* scenario considered the possibility of both unintentional and deliberate manmade incidents that disable communications between the public and the PSAP facilities. The main risk presented was theft or destruction to the facility and related infrastructure. Theft of copper wire was largely the main risk addressed. In the event that charged copper wire was stolen, the consequences could be significant; thieves could be at risk for injury or death due to contact with live electrical lines, and emergency communications services between citizens and authorities and authority-to-authority could be disrupted or disabled. The time required for re-establishing connectivity could be significantly delayed while the location of the disruption is being sought and its cause investigated. Other possible scenarios include direct attacks to the PSAP facility and related infrastructure, as well as accidental incidents resulting in physical damage to the facility and related infrastructure.

Of the risks presented, improving physical security to the PSAP facility and related infrastructure offers significant mitigation to reduce these risks. Some key physical security practices include—

- **Fencing and Gates**-The basic practice of establishing fence lines and gates to protect the perimeter of a PSAP or other communications infrastructure from unauthorized access to the facility and infrastructure will serve is a key preventative step.
- **Alarm/Surveillance Systems**-Systems with motion and magnetic sensors will aid in protecting ground where a human cannot be physically present to supervise access. The use of audible alarms that activate upon tripping a sensor will act as a first stage of deterrence. Use of surveillance systems enables a smaller amount of human operators to protect a greater area and to record any unauthorized access or attempts to tamper with the facility or infrastructure site as it is occurring. The ability to protect an entire facility without the need for human presence is offered.
- **Human Presence (Guards)**-Staffing a facility with dedicated security personnel affords the opportunity for surveillance and alarm system monitoring and fast response in the event of an attack or incident. Security personnel on site can provide improved response times to any unauthorized access or tampering detected. In the event of a malicious attack, the fast response and presence of a human guard can increase the defense of the facility. Without human presence onsite, the likelihood of a delayed response is increased, subject to the availability and location of area law enforcement.

In addition to these key physical security practices, protecting the ESS critical infrastructure from tampering, damage, or disruption is important. Fencing and gates require maintenance and inspection to ensure that the perimeter remains sound. Surveillance of fence lines and gates can help provide redundancy to ensure that tampering is not taking place, and gates can be equipped with supervisory alarms to signal their use. Any alarms or surveillance systems will require uninterrupted power supplies to be viable around the clock. As mentioned in the risk assessment, manmade unintentional or deliberate attacks can also come from insider threats. No fence, gate, or alarm system will effectively protect a facility if unauthorized persons or disloyal insiders are permitted access. This may require that a formal background investigation or other screening process be in place for persons with access to the communications center and infrastructure sites, including commercial service providers who may respond to maintenance and repair requests at these sites.

2.3.2 The Impact and Feasibility of Improved Public Safety Answering Point Physical Security Measures

Implementing physical security measures for PSAP facilities and infrastructure specifically addresses the risk of copper wire theft and/or physical damage or destruction to the facility or its related infrastructure. Improving the physical security of cyber infrastructure will decrease the extent of exposure of the vulnerabilities but will have no effect on the consequences of exploitation. Improved physical security measures were the only risk response to this scenario that significantly reduce vulnerabilities from medium to low, but these measures did not lessen the consequence of an event, should one occur. This is depicted in Figure 7 on the following page.

Figure 7. Estimated Level of Cyber Risk to PSAP Facilities and Related Infrastructure, as Depicted by the Red Block. Cyber risk analysis indicates, via the blue block, that the reduction of the likelihood of threat exploiting the vulnerability in the event of a manmade-unintentional scenario. Implementation of physical security measures will reduce the likelihood of a manmade-unintentional scenario to a negligible level.

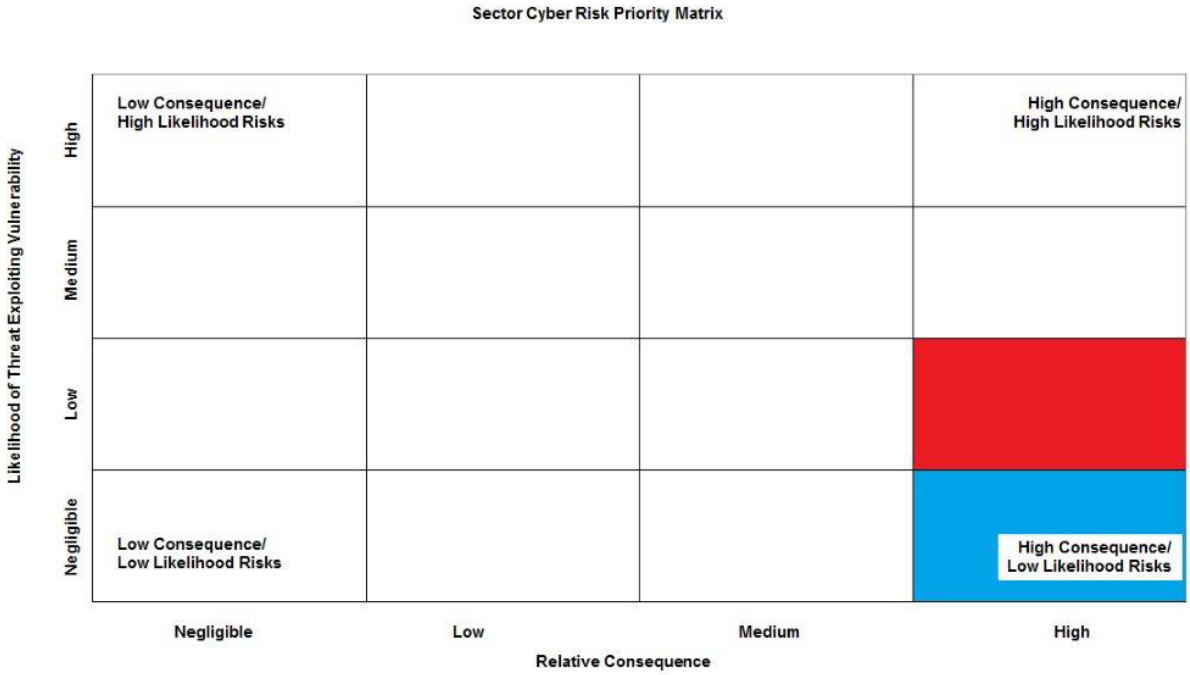
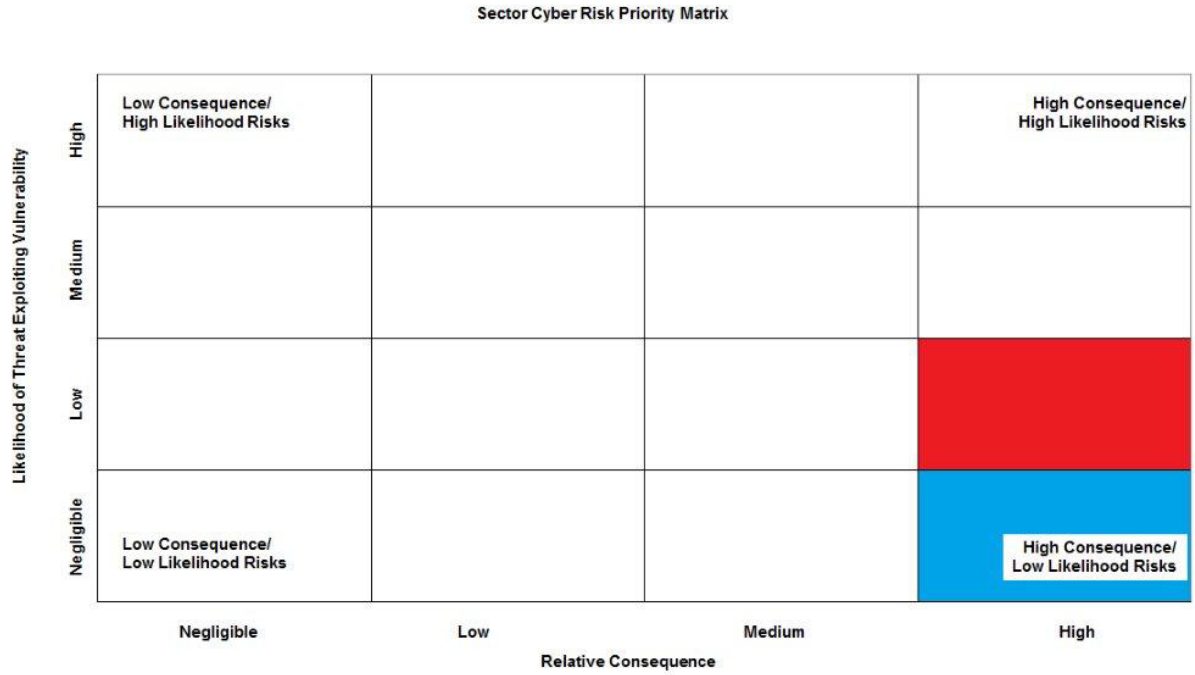


Figure 8 on the following page shows a risk reduction from an unintentional manmade scenario accomplished by implementing increased physical security measures at PSAP facilities.

Figure 8. Estimated Level of Cyber Risk to PSAP Facilities and Related Infrastructure, as Depicted by the Red Block. Cyber risk analysis indicates, via the blue block, a reduction of the likelihood of threat exploiting the vulnerability during a manmade- unintentional scenario. Implementation of physical security measures will reduce the likelihood of a manmade-unintentional scenario to a negligible level.



The implementation of physical security measures can provide some challenges, depending on the complexity of the practice desired. However, the feasibility of this implementation is improved by its modest costs and time commitment. This response can be likely completed in less than 2 years.

2.3.3 Organizational Responsibilities for Implementing Improved Physical Security Measures at Public Safety Answering Point and Communications Infrastructure Facilities

A PSAP or communications service agency serving ESS agencies should pursue the implementation of improved physical security measures as an effective cyber risk reduction effort. The key leaders overseeing this effort may be a PSAP director, an emergency communications center manager, or a radio system manager. If the agency or jurisdiction has a facility security officer, this person may assume the key leadership role. The important point is that the key leader should have knowledge about the existing policies and procedures for protecting physical and cyber infrastructure and the authority to make decisions to improve physical security where needed. Understanding the baseline physical security in place already and whether any redundancies in that baseline exist will also be important.

Table 6 on the following page depicts the structure needed to successfully address and consider viable options to implementation and risk reduction.

Table 6. Cyber Risk Mitigation Using Improved Physical Security Measures.

Implementing Improved Physical Security Measures at PSAP and Communication Infrastructure Facilities
Key authority or group:
Varies by jurisdiction; Federal or state telecommunications manager, the state 9-1-1 or PSAP Coordinator, local or tribal communications service provider, information technology manager, or radio system manager • Assess public and political support needed to acquire physical security technologies. • Make decisions to upgrade physical security and align policies with new practices. • Identify funding sources to finance acquisition and operation.
Primary Organizational Responsibility:
Varies by jurisdiction; Federal or state telecommunications manager, the state 9-1-1 or PSAP Coordinator, local or tribal communications service provider, information technology manager, or radio system manager that operates and maintains the PSAP and communications infrastructure facilities • Collaborate with local exchange carriers serving the affected infrastructure sites to discern the cost and availability of route diversity. • Develop requirements for diversity in communications infrastructure sites; these will be variable based on whether a PSAP is operated by the key authority or if other communications centers and supporting communications infrastructure, such as land mobile radio networks, must be supported. • Identify COOP sites or other infrastructure sites that could be used to establish facility diversity for tower sites and other communications infrastructure. • Assess the suitability of identified sites for development as a diverse facility for communications system support.
Secondary Organizational Responsibilities:
Operating PSAP facilities • Engage in the development of policies, practices, and procedures that will support the implementation of physical security measures. • Develop training and exercises needed to develop proficiency in operation the new technology. • Make decisions to upgrade physical security and align policies to new practices
Finance/administrative aspects of the PSAP • Ensure that legal and policy support and fiscal resources are available and can be authorized to purchase security related personnel and equipment. • Identify funding sources to finance acquisition and operation
Logistical support • Procure necessary equipment and furnishings based on operational requirements and the administrative/finance organization's prior approval. • Provide any logistics needed to support implementation of new mitigations.

As indicated above, there is little or no direct Federal influence involved or required to implement the measures presented. Decisions on which cyber risk mitigation mitigations to implement and how to implement them will be made and executed at the governmental level of the entity shown to be at risk.

2.4 Adopt and Implement Rollover Capabilities in Public Safety Answering Point and Emergency Operation Center Facilities

Overloaded communications networks can occur as a result of a malicious actor launching a denial of service attack or as a result of unintentional factors, such as a sudden or

unexpected surge in public use. Establishing rollover capabilities in potentially vulnerable PSAP and EOC facilities acts as a redundant back-up system so that service disruptions can be minimized or eliminated in the event of an incident.

2.4.1 Addressing Cyber Risks through Rollover Capabilities in Public Safety Answering Point and Emergency Operation Center Facilities

The ESS Cyber Working Group suggests that developing rollover capabilities would significantly reduce the overall consequences associated with network overload. Rollover, a term used most often in legacy Basic and Enhanced 9-1-1 systems is a form of call congestion management that controls traffic when there are insufficient resources to meet demand, such as when there are more requests for calls than there are lines available to deliver them. It may be achieved by rejecting requests, or diverting calls.

In the *ESS CRA*, one of the scenarios evaluated deliberate and unintentional manmade threats that could result in the loss or degradation of 9-1-1 and other emergency mobile communications. Loss of communications could also result in the inability to deploy resources, the loss of public confidence in emergency services, and/or confusion and panic. In the context of cyber risk mitigation, rollover allows relief from these consequences by routing calls to another PSAP or EOC facility to handle the excess demand or providing for call processing when there is an outage at the primary PSAP facility due to manmade intentional or unintentional threats. Several of the infrastructure vulnerabilities evaluated include open access rights and deliberate or accidental manipulation of equipment. In worst case scenarios, ESS services could be unavailable to citizens until normal capabilities became available again. Rollover capabilities could provide uninterrupted access during this loss of network service.

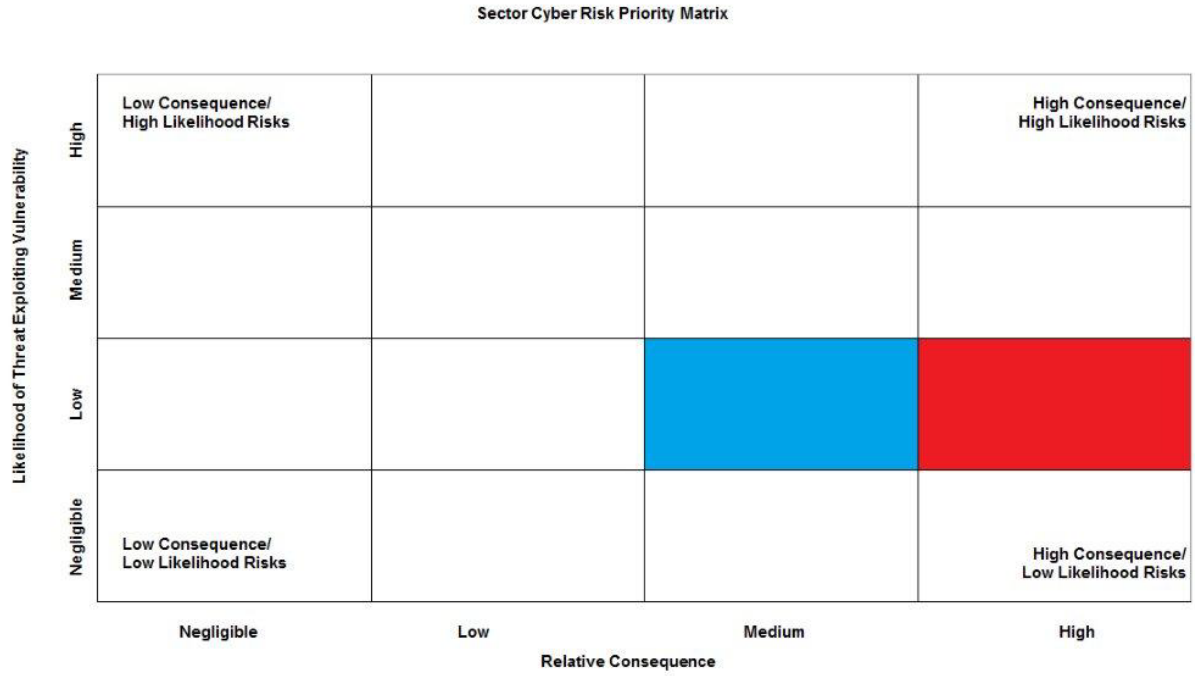
2.4.2 The Impact and Feasibility of Public Safety Answering Point and Emergency Operation Center Facility Rollover Capabilities as a Cyber Risk Reduction Measure

Regarding the impact that rollover capabilities would have on cyber risk, this mitigation measure was seen to effectively reduce the consequences of cyber threats from high to medium levels. The feasibility of this measure has not yet been fully vetted. For example, intergovernmental agreements (automatic or mutual aid) of the sort described on pages 20, 29, and 30 are widely used and available, but those needed to support rollover capabilities have not been executed to any great extent to date. The legal and political support for such agreements exist, but some thought as to the mechanisms to activate these agreements, duration of rollover operations, responsibility for associated costs (for personnel surge, technology switches, and information management and dissemination, as examples), and compatibility between PSAP facilities would be required before these agreements could be developed and signed.

Implementation of rollover capabilities address both deliberate and unintentional manmade risks identified in the *ESS CRA* scenario. Regarding deliberate manmade threats, the evaluation showed that developing rollover capabilities in PSAP and EOC facilities will slightly reduce the extent of vulnerability exposure to communication networks. However, rollover capabilities will significantly reduce the consequence of exploitation to medium (as shown in Figure 9 on the following page), particularly with respect to the economic security of the affected area. Establishing automatic or mutual aid agreements in advance and developing

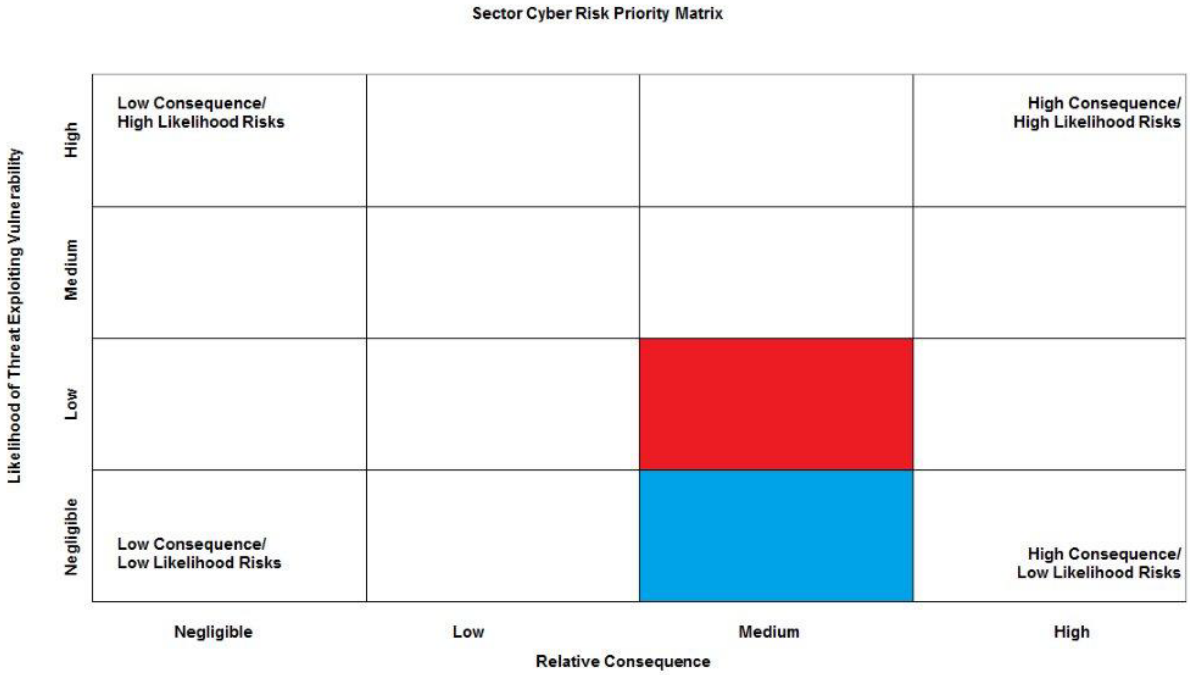
rollover capabilities to re-route calls to an alternate PSAP reduces what was evaluated as a very high-consequence cyber threat in the *ESS CRA* to a medium risk. Thus, establishing rollover capabilities is a significant cyber risk mitigation measure.

Figure 9. Estimated Level of Cyber Risk to Overloaded Communications Network, as Depicted by the Red Block. Cyber risk analysis indicates, via the blue block, that the reduction of cyber risk that could be realized if rollover capabilities for PSAP and EOC facilities were implemented as a mitigation measure against a manmade-deliberate threat.



Regarding an unintentional manmade threat, evaluation of the risk response showed that developing rollover capabilities in PSAP and EOC facilities will slightly reduce likelihood and consequences. However, developing rollover capabilities significantly reduces the overall consequence of exploitation (as shown in Figure 10 on the following page), particularly with respect to the adverse financial costs associated with the loss of communications networks, regardless of the threat.

Figure 10. Estimated Level of Cyber Risk to Overloaded Communications Network, as Depicted by the Red Block. Cyber risk analysis indicates, via the blue block, that the reduction of cyber risk that could be realized if rollover capabilities in PSAP and EOC facilities were implemented as a mitigation measure against manmade-unintentional threats.



Rollover capabilities do provide both implementation and operational challenges, and these capabilities face constraints related to local and state legal and political frameworks. The financial costs of rollover capabilities may be largely due to the need for facilities, staff, training, and technology resources. The technology and compatibility of existing systems may also hinder implementation when trying to develop an alternative and compatible facility with new technology. The most significant constraint to implementation may come from the organization's culture and the nature of compliance. Some jurisdictional PSAP and EOC leaders may have difficulty justifying adding rollover capabilities that may only be used in response to an unforeseen incident. Political or policy leaders may be unfamiliar with the circumstances that could create the need for rollover capabilities, and if a given agency has not experienced this need to date, advocating for a proactive (rather than reactive) measure may be a challenge. This cyber risk mitigation is a long-term measure with significant implementation time required and may take 2 years or longer to implement.

2.4.3 Organizational Responsibilities for Implementing Rollover Capabilities in Public Safety Answering Point and Emergency Operation Center Facilities

This cyber risk mitigation measure will involve multiple agencies, and as such, it is likely that political leaders (possibly elected officials) and agency heads may need to foster the pursuit of this mitigation. Organizations should address actions needed to implement rollover capabilities via an inter-organization team, although 9-1-1 coordinators and relevant chief

information officers will also play an important role. The key authority should assess the political support needed to acquire new capabilities and should identify the funding sources to finance new acquisitions and operations.

Additional actions that should be taken to support implementing rollover capabilities in PSAP and EOC facilities can be found in Table 7 below.

Table 7. Cyber Risk Mitigation Using Rollover Capabilities in PSAP and EOC Facilities.

Implementing Rollover Capabilities for Cyber Risk Mitigation
Key authority or group:
Varies by jurisdiction; state 9-1-1 Coordinator, city manager, county CIO, regional 9-1-1 authority, etc. are all possibilities • Assess public support and the political capital needed to acquire and support rollover capabilities. • Identify funding sources to finance acquisition and operation.
Primary Organizational Responsibility:
9-1-1 services planning body; At the local or state level, this may be the state 9-1-1 coordinator, a 9-1-1 service authority, or other organization • Involve state 9-1-1 coordinators in any methods or measurement of implementation. • Reach to Federal resources for guidance. The National 9-1-1 Program at USDOT/NHTSA is a likely source for planning support. • Research the work of the FCC, which has been working with telecommunications service providers and local exchange carriers on the resilience of telephone networks in the face of natural disasters. For example, the FCC has done work with Verizon® and AT&T® related to major power outages during derecho storms, and lessons learned therein may be useful. • Determine if existing telephone technology supports transferring calls automatically to other facilities or if new technology is needed.
Secondary Organizational Responsibilities:
Operating PSAP facilities • Develop policies, practices, and procedures that will support rollover implementation, and initiate training necessary to ensure it is properly operated. • Develop training and exercises needed to become proficient in executing rollover procedures, including the activation of alternate PSAP facilities and the activation/deactivation of rollover agreements.
Finance/administrative aspects of the PSAP • Ensure that legal and policy support and fiscal resources are available and can be authorized to engage in such exercises and agreements.
Logistical support • Procure necessary equipment and furnishings based on operational requirements and the administrative/finance organization's prior approval. • Provide any logistics needed to support the activation of rollover agreements or to conduct training and exercises on failover procedures.

As indicated in Table 7 above, there is low Federal engagement and influence required to implement rollover capabilities in PSAP and EOC facilities. Specific requirements and constraints will vary by jurisdiction, but most of the progress and constraints will concentrate at the local and state levels.

3 PLANNING AND PREPARING FOR CYBER INCIDENTS

This segment of the Roadmap provides mitigation measures that will assist ESS agencies in developing plans and preparations to reduce cyber risk.

3.1 Conduct and Evaluate Failover Capabilities through Exercises

The ESS Cyber Working Group suggested that conducting regular exercises to test failover capabilities and then regularly evaluating results from exercises can minimize the risk of a disabled 9-1-1 service center due to a natural disaster or other debilitating scenario. As noted on page 12, the consequences of the loss or degradation of 9-1-1 capabilities can cascade across several different critical infrastructure sectors and can significantly affect the ability of ESS to perform emergency response.

3.1.1 Addressing Cyber Risks through Failover Exercises

Failover exercises, in which a lost or damaged facility can be simulated, are more easily executed in a Next Generation 9-1-1 environment; for instance, authorized and enabled technologists can re-route calls more simply. Furthermore, during stead-state operations, the primary agency can test routing systems and switches with a partnering agency or an alternate PSAP to discern whether an actual loss of connectivity or a damaged facility could be quickly and effectively addressed. Nonetheless, failover exercises can also be developed and executed for Basic or Enhanced 9-1-1 systems and services as well.

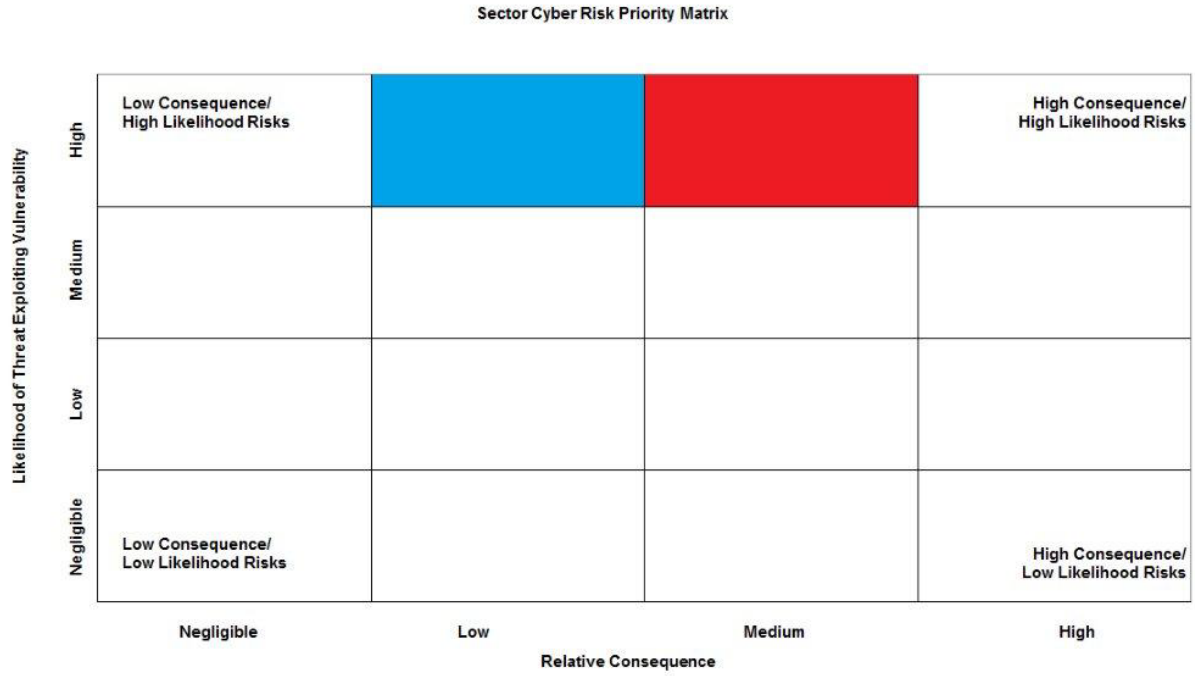
Failover exercises can help manage consequences by ensuring that sector personnel are equipped to respond to incidents. Benefits of these exercises include:

- Practicing failover transitions from a disabled system to a redundant back-up system can reduce confusion and delay during an actual emergency situation.
- Establishing roles and responsibilities during exercises enables all participants to successfully complete their required task to ensure an efficient transition.
- Consecutive implementation of Next Generation 9-1-1 and activation of back-up PSAP or EOC facilities with failover exercises increases the likelihood of a smooth transition from the affected facility to the reserve facility, reducing the time of unavailable 9-1-1 services.

3.1.2 The Impact and Feasibility of Failover Exercises as a Cyber Risk Reduction Measure

The mitigation of failover exercises will moderately decrease the potential consequences. Implementation will have no effect on overall likelihood of the natural disaster but will moderately decrease consequences, particularly related to public health and public confidence because of the minimized delay in 9-1-1 services. On the following page, Figure 11 depicts the level of risk reduction that conducting regular failover exercises would provide.

Figure 11. Estimated Level of Cyber Risk to ESS Infrastructure from a Natural Disaster, as Depicted by the Red Block. Cyber risk analysis indicates, via the blue block, the reduction of cyber risk that could be realized if failover exercises were regularly conducted as a mitigation measure.



Overall feasibility of implementing failover exercises is high since exercises are a widely practiced element of ESS operations and face little to no cultural barriers to adoption. However, limited political issues and financial costs involved with activating a back-up center to test during exercises, as well as introducing additional staff during an exercise, may present moderate constraints to implement. The plan for implementation should include adjusting annual training calendars (varying by jurisdiction and state) to include failover exercises. Implementation may also require gaining political support and financial resources for staff relocation and center activation. This mitigation measure can likely be completed in a relatively short timeframe of 9 to 12 months, given the established culture of exercises in the sector.

3.1.3 Organizational Responsibilities for Instituting Failover Exercises

Responsibility for incorporating failover exercises into a given jurisdiction's training cycle will mostly be at local or state level with the organization operating 9-1-1 facilities. Failover exercises will require strong leadership to develop and execute as they involve expending funds for planning, staffing, and personnel coverage, as well as potential costs for mobilizing personnel. There will be concerns about missing actual calls, and careful coordination is required with the local exchange carriers to ensure that calls are not dropped due to a technical oversight. Table 8 on the following page depicts how such a key authority or group could delegate responsibilities for designing and executing failover exercises and training.

Table 8. Cyber Risk Mitigation Using Failover Exercises.

Conducting Failover Exercises for Cyber Risk Mitigation
Key authority or group:
Varies by jurisdiction; state 9-1-1 Coordinator, city manager, county CIO, regional 9-1-1 authority, etc. are all possibilities • Assess public support and the political will to acquire funding for staff relocation and reserve center activation.
Primary Organizational Responsibilities:
Operating PSAP facilities • Develop training and exercises needed to become proficient in executing failover procedures, including the activation of alternate PSAP facilities and the activation/deactivation of rollover agreements.
Finance/administrative aspects of the PSAP • Ensure that legal and policy support and fiscal resources are available and can be authorized to engage in such exercises and agreements.
Logistical support • Procure necessary equipment and furnishings based on operational requirements and the administrative/finance organization's prior approval. • Provide logistics needed to support the activation of rollover agreements or to conduct training and exercises on failover procedures.
Secondary Organizational Responsibilities:
9-1-1 services planning body; at the local or state level, this may be the state 9-1-1 coordinator, a 9-1-1 service authority, or other organization • Involve state 9-1-1 coordinators in any methods or measurement of implementation. • Research the work of the FCC, which has been working with telecommunications service providers and local exchange carriers on the resilience of telephone networks in the face of natural disasters. For example, the FCC has worked with Verizon® and AT&T® related to major power outages during derecho storms, and lessons learned therein may be useful.

As indicated above, there is little or no Federal engagement and influence involved in designing and executing failover exercises.

3.2 Establish Comprehensive Cybersecurity and Continuity of Operations Plan Implementation Training and Exercises for Staff

Cybersecurity and COOP plans are essentials to every public safety agency. Regardless of the cyber resources they use—voice, data, or video systems and networks—in their day-to-day business, there are basic plans in place to guide the use of these resources, and most of these systems and networks are supported by COOP plans to ensure the availability of resources during incidents. Such plans may be as simple as using manual operations to emergency services and then converting or "catching up" the data into automated or cyber-based systems and networks once service is restored. They may also be more elaborate, such as Information Technology Disaster Recovery Plans. The level of sophistication that is necessary should be based on the criticality that each cyber resource plays in the delivery of emergency services or to the critical business functions (such as payroll, training and certification databases, or criminal justice information systems) that must be supported for the success of the organization.

Plans should address normal operating conditions and triggers that would cause a deviation from those conditions, such as power outages or the lack of availability of a database. An agency's plans may call for a variety of measures, such as requiring that redundant data should be readily available for emergency purposes. Whether the resulting data inaccessibility is intentional or unintentional, the procedure for restoring systems access is the same.

Training and education lays the path for successful and fast response to the loss of access to data necessary to maintain full functions and also helps to prevent incidents of lost data access through better trained and more mindful employees. More sophisticated plans may include the development of advanced COOP measures, such as maintaining a "hot" COOP site, as discussed on page 48. In this instance, a Hot COOP site would have alternate access paths to databases in use in the primary facility so that a loss of the primary access path would not prevent access to the database from the COOP site. Ensuring smooth operation and transfer of duties from the primary site to the Hot COOP site requires training and exercises. Training and exercises also help reduce the risk of incidents that require Hot COOP transfer by better educating employees on how to safely use cyber resources, which result in fewer accidents and promote a broader ability to sense internal threats.

3.2.1 Addressing Cyber Risks through Comprehensive Cybersecurity and Continuity of Operations Plan Implementation Training and Exercises for Staff

The *ESS CRA* pointed out that "ESS databases are critical to supporting sector missions and activities. Should a database be unavailable, there will be disruption to mission capabilities within and across ESS disciplines. Databases are vulnerable to cyber-attack and subject to manmade deliberate and unintentional threats." That latter scenario in which a database is vulnerable to a cyber-attack serves as a driver for developing cybersecurity and COOP plans that guide the organization when lost availability of an important database occurs. Developing cybersecurity and COOP plans has limited benefit to ESS organizations unless those plans are well-known and well-understood by those who will rely on them when access to an important cyber resource is lost. It is essential, then, that ESS personnel receive training on their organization's cybersecurity and COOP plans and conduct exercises in implementing those plans. The benefits of conducting comprehensive cybersecurity and COOP plan training and exercises for ESS personnel include:

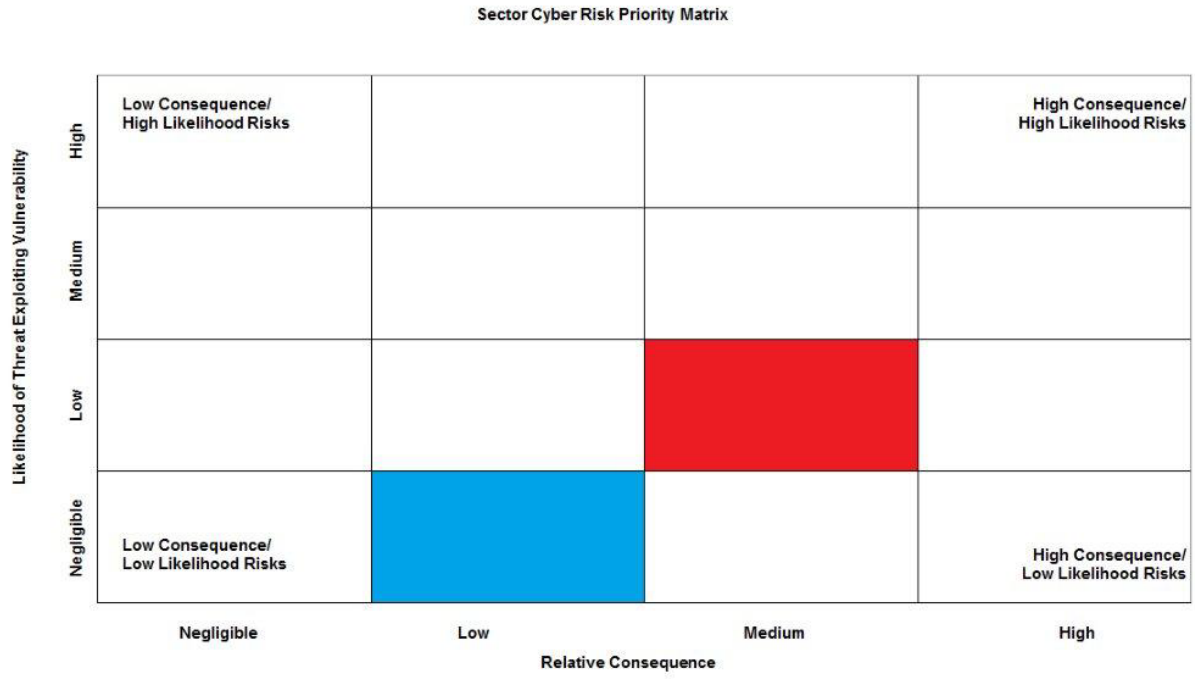
- **Developing Preparedness Knowledge**-Preparing ESS personnel to create the notifications and take the steps necessary to respond to the situation that has caused the lost access or impairment. This effort helps reduce confusion about what to do and when and minimizes the disruption caused when cyber resources on which ESS personnel rely are suddenly unavailable. ESS personnel will know what to do and can move forward with those actions.
- **Developing Continuity Skills**-Training and exercising ESS personnel on continuity plans helps them to react appropriately when a cyber resource is unavailable, reduces confusion about what to do when such a situation is encountered, and permits the organization to quickly transition from routine to COOP activities and back.
- **Developing Cognitive Abilities**-Developing the ability to recognize when access to a database or other cyber resource is not available or is otherwise impaired is important to trigger repair and restoration work and to minimize downtime for any cyber resource.

Training and exercises helps ESS personnel gain proficiency in recognizing triggers and ensures that they can act quickly to implement plans. This permits a more rapid response to the circumstances, resulting in minimized disruption of service delivery. This rapid response also fosters a strong recovery effort that ultimately results in a restoration of cyber resource services and prevents or minimizes information loss.

3.2.2 The Impact and Feasibility of Comprehensive Cybersecurity and Continuity of Operations Plan Implementation Training and Exercises for Staff

An evaluation of this risk mitigation measure revealed that instituting training and exercises would moderately reduce the overall risk that a lack of access to a database poses to the sector. Training and exercises would make databases less vulnerable to an intentional act of disruption, but a determined attacker may still bypass well-trained employees. Training and exercises would slightly reduce a database's vulnerability in the case of an unintentional incident, as better trained employees would be less likely to cause accidents that cause the database to become unavailable. Given that these measures are mostly preventative, they would modestly reduce the consequences of an attack. Training and exercises provide a greater likelihood of reducing the risk of a deliberate threat than an unintentional threat, as portrayed in Figure 12 below.

Figure 12. Comprehensive Cybersecurity and COOP Plan Implementation Training and Exercises for Staff Provide a Greater Reduction in Consequences of an Unintentional Manmade Act to Prevent Access to an ESS Database than It Does for Intentional Acts.
Providing comprehensive training and exercises may slightly reduce the likelihood of an intentional act from occurring by raising awareness of the potential and educating ESS personnel on the circumstances that may help them recognize when an intentional act has taken place.



It is highly feasible to use training and exercises to address cybersecurity and COOP plan implementation. ESS personnel are well-conditioned in using training to promote preparedness on an individual- and agency-level to conduct their missions in routine and unusual circumstances. It is part and parcel of this sector's culture to conduct training and to execute exercises to build and develop knowledge, skills, and abilities. COOP planning varies widely across the ESS; some agencies have been proactive in developing crisis plans, and they may have had some level of business continuity planning to ensure that key business functions can continue if the supporting cyber resources are lost. However, some agencies regard COOP planning as little more than having an insurance policy in place to cover physical losses of real or capital property, as shown in a U.S. Fire Administration report[6] on the subject as it related to fire and emergency services organizations. While the focus of this report is on cybersecurity threats, risks, and losses that were not addressed in that topical report, it is important to note that the number of ESS agencies that have developed Cold, Warm, or Hot COOP sites is limited.

The factor that may inhibit this cyber risk mitigation measure is the cost. Training and exercises can be conducted at a manageable cost, given that it is fairly easy to create a scenario in which access to a cyber resource is unavailable and that the scale of the scenario—and thus, its financial impact—can be tailored to minimize disruptions. The development of actual Cold, Warm, and Hot COOP sites is an altogether different cost to consider. Such sites, especially Hot COOP sites, can be very costly. This is primarily due to the costs of staffing an additional facility with a sufficient cadre of qualified personnel, but it is also due to the capital costs associated with the development of a site, equipping it, operating it, and maintaining it on a full-time, year-round basis.

The fiscal impacts can be addressed in a number of ways. A Hot COOP site could be shared among multiple ESS agencies or could provide service for a number of agencies in a political jurisdiction, for example, and some duties could be directed to that location to make maintaining staff onsite a more justifiable expense. Each ESS organization will have to consider its fiscal resources and determine what is and is not acceptable in approaching this cyber risk mitigation measure.

3.2.3 Organizational Responsibilities for Comprehensive Cybersecurity and Continuity of Operations Plan Implementation Training and Exercises for Staff

The key authority or group overseeing the implementation of a comprehensive cybersecurity and COOP plan implementation training and exercise effort will vary depending upon the level of government involved. Federal agencies must develop COOP plans because of Presidential Decision Directive 8– National Preparedness (PPD-8). According to PPD-8, "This directive is aimed at strengthening the security and resilience of the United States through systematic preparation for the threats that pose the greatest risk to the security of the Nation, including acts of terrorism, cyber-attacks, pandemics, and catastrophic natural disasters. Our national preparedness is the shared responsibility of all levels of government,

[6] A 2001 topical report, the last one that the U.S. Fire Administration (USFA) issued on the subject, indicated that the vast majority of fire service facilities and their contents (mobile apparatus, tools, equipment, protective firefighter ensembles, etc.) are either uninsured or under-insured. This report does not address other COOP planning aspects to prepare organizations or to ensure continuity of operations.

the private and nonprofit sectors, and individual citizens. Everyone can contribute to safeguarding the Nation from harm. As such, while this directive is intended to galvanize action by the Federal Government, it is also aimed at facilitating an integrated, all-of-Nation, capabilities-based approach to preparedness."[7]

PPD-8 directs that the key authority for its implementation lies with the Secretary of the U.S. Department of Homeland Security. At the state or territorial level, the key authority may be the state's secretary for homeland security or equivalent, such as an adjutant general over emergency management and disaster preparedness. At the tribal or local levels, the key authority may be the leading local elected official or an appointed leader, such as a city manager, a county's chief information officer, or an emergency service agency's information technology manager. Table 9 on the following page depicts how such a key authority or group could delegate responsibilities for developing, acquiring, and implementing comprehensive cybersecurity and COOP plan implementation training and exercises.

[7] Presidential Policy Directive 8, National Preparedness (Mar. 30, 2011) is available online at http://www.dhs.gov/presidential-policy-directive-8-national-preparedness.

Table 9. Cyber Risk Mitigation through Comprehensive Cybersecurity and COOP Plan Implementation Training and Exercises.

Implementing Rollover Capabilities for Cyber Risk Mitigation
Key authority or group:
Varies by jurisdiction; state or local Homeland security secretary or director, state adjutant general, city manager, county CIO, agency-specific cybersecurity or COOP planners are all possibilities • Assess sufficiency and availability of cybersecurity and COOP plans. • Identify funding sources to finance plan implementation training and exercises.
Primary Organizational Responsibilities:
Cybersecurity and COOP planning body; at the local or state level, this may be the homeland security or emergency management agency, the information technology service provider, or another organization • Reach to Federal resources for guidance. The DHS Office of Cybersecurity and Communications' Strategic Engagement for Cyber Infrastructure Resilience is a likely source for planning support. The Federal Emergency Management Agency (FEMA) offers training on developing exercises at a number of levels of engagement to help agencies tailor their exercise needs to their funding and staffing resources.
Secondary Organizational Responsibilities:
Operating PSAP facilities • Develop training and exercises needed to become proficient in executing COOP plans. • Execute exercises and, using key objectives (such as meeting time-to-implement goals, accomplishing transfer of staff, or activating backup systems), evaluate the ability of staff to transition between routine operations and complete COOP plan implementation.
Finance/administrative aspects of the PSAP • Ensure that legal and policy support and fiscal resources are available and can be authorized to engage in such exercises.
Logistical support • Procure necessary equipment and furnishings based on operational requirements and the administrative/finance organization's prior approval. • Provide any logistics needed to support activation of COOP plans or to conduct training and exercises on failover procedures.

As indicated above, there are some Federal engagements and influences in developing comprehensive cybersecurity and COOP training and exercises for staff. In addition to the cybersecurity programs mentioned, the Federal Emergency Management Agency offers training on developing and executing a variety of homeland security exercises, including COOP or business continuity plan execution.

3.3 Create Hot Continuity of Operations Sites with Database Backups

The ESS Cyber Working Group suggested that creating Hot COOP sites with database backups can minimize the risk of a disabled 9-1-1 service center due to a natural disaster or other debilitating scenario. A Hot COOP site, as discussed in the footnote on page 16, is a secondary site that would provide alternate access to databases in the primary facility, so a loss of the primary access path would not cut off all access. Ensuring smooth operation and transfer of duties from the primary site to the Hot COOP site requires training and education. Training and education also help to reduce the risk of incidents requiring Hot COOP

transition, since better educated employees are reminded how to conduct their work safely and accurately and to stay aware of potential insider threats.

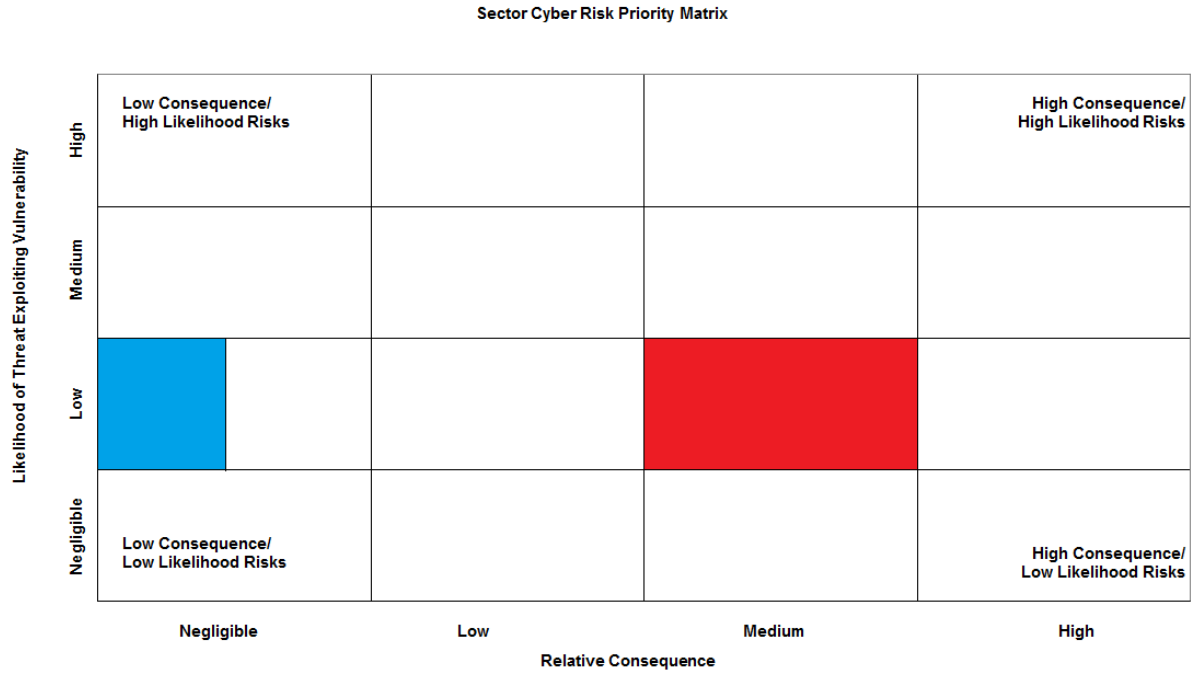
3.3.1 Addressing Cyber Risks through Hot Continuity of Operations Sites

The *ESS CRA* evaluated manmade deliberate and unintentional threats that could result in the compromise of, disruption of, redirection of, or damage to sensitive criminal investigations; the unauthorized access to nationally connected networks; unfavorable media exposure and/or loss of public trust; or denial of sensitive data access—including National Crime Information Center (NCIC) access— to authorized users. Vulnerabilities that could contribute to this scenario include susceptibility to a network breach through the software or application layer, insufficient security procedures, open access rights, and database corruption.

3.3.2 The Impact and Feasibility of Hot Continuity of Operations Sites as a Cyber Risk Reduction Measure

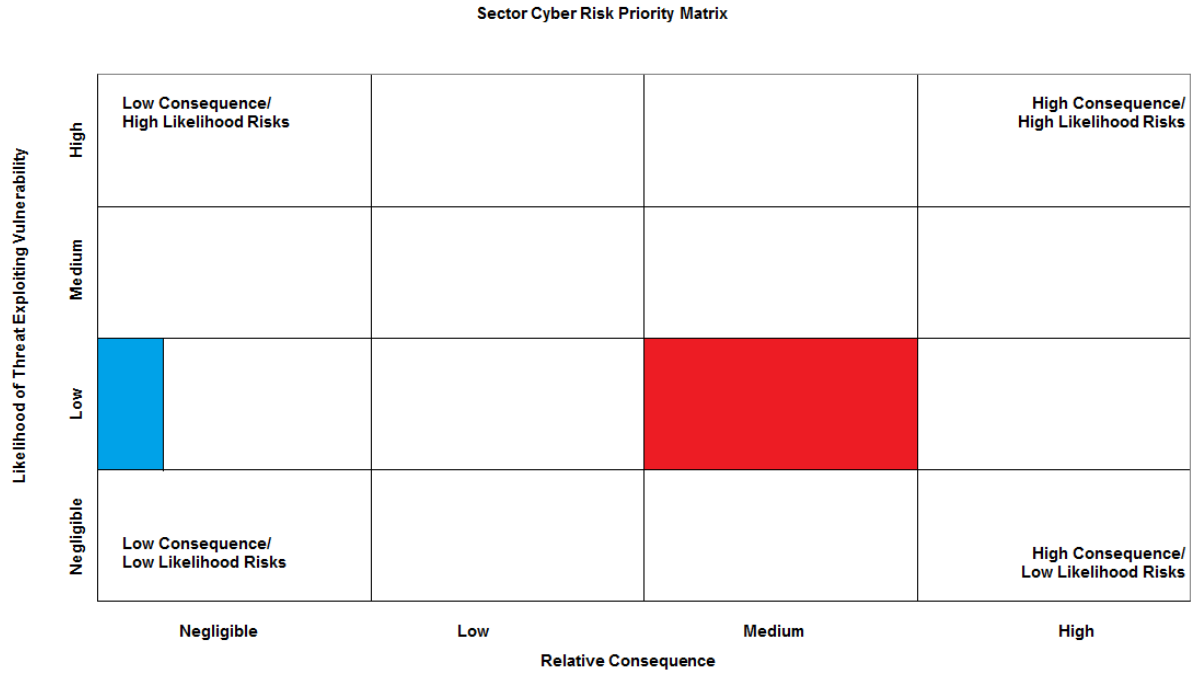
Implementing Hot COOP sites will not affect the likelihood of a deliberate manmade threat exploiting a vulnerability or of an unintentional manmade incident but will significantly lower consequences to a negligible level. The *ESS CRA* noted that consequences of an unintentional disruption can be slightly higher than consequences of a deliberate disruption depending on the database in question. This discrepancy can occur due to constraints on deliberate actors or because of the longer time lapse before an unintentional disruption is identified. In sum, Hot COOP sites will significantly reduce the consequences of either a deliberate or unintentional manmade event, reducing overall consequences from high to nearly negligible. Establishing or maintaining Hot COOP sites would also enable a database to continue functioning with limited interruption. Figure 13 on the following page depicts the level of risk reduction that creating a Hot COOP site would provide in response to a deliberate threat.

Figure 13. Estimated Level of Cyber Risk to ESS Infrastructure from a Deliberate Manmade Threat, as Depicted by the Red Block.
Cyber risk analysis indicates, via the blue block, that the significant reduction of cyber risk that could be realized if Hot COOP sites are established as a mitigation measure. A Hot COOP site cannot reduce the likelihood of a deliberate threat, but it can significantly reduce consequences from a medium to a negligible level.



Moreover, Figure 14 on the following page depicts the level of risk reduction obtained in response to an unintentional threat.

Figure 14. Estimated Level of Cyber Risk to ESS Infrastructure from an Unintentional Manmade Threat, as Depicted by the Red Block.
Cyber risk analysis indicates, via the blue block, that cyber risk could be significantly reduced if Hot COOP sites were established as a mitigation measure. A Hot COOP site cannot reduce the likelihood of a deliberate threat, but it can significantly reduce consequences from medium-high to a negligible level.



Overall feasibility of creating a Hot COOP site is constrained by the high financial cost and time required to implement—possibly 24 months or longer—before a site is fully operational. Current market conditions and potential political constraints may also be detrimental to implementation because significant capital investment is required to activate a new Hot COOP site and could mean diverting resources from competing efforts. Emergency services personnel can communicate the value proposition of Hot COOP sites to policymakers and area representatives and can influence political priorities, but this process could constrain implementation. In the end, even if establishing a Hot COOP site is unfeasible, emergency services organizations should work to establish COOP capabilities at alternate sites, either Warm or Cold, to permit devolution if a COOP plan is activated.

3.3.3 Organizational Responsibilities for Approving, Activating, and Sustaining Hot Continuity of Operations Sites

Table 10 on the following page depicts how such a key authority or group could delegate responsibilities for deciding whether to create and activate a Hot COOP site. Strong leadership is required to determine whether and how to pursue this cyber risk mitigation measure. There is considerable planning and development required to establish a Hot COOP site, and such sites are usually expensive to establish, maintain, and operate. According to the analysis, a Hot COOP site can minimize the consequences of a disabled 9-1-1 center by providing redundancy, but there must be a prior analysis of the investment justification to discern if the return on investment can be met.

Table 10. Cyber Risk Mitigation Using Hot COOP Sites.

Conducting Failover Exercises for Cyber Risk Mitigation
Key authority or group:
Varies by jurisdiction; state 9-1-1 Coordinator, city manager, county CIO, and regional 9-1-1 authority are all possibilities • Assess public support and the political will to acquire funding for staff relocation and Hot COOP site location and activation. • Identify funding sources to finance maintenance and operations. • Assess whether the jurisdiction currently operates an existing COOP site (Hot, Cold, or Warm). • Verify whether the organization or jurisdiction currently has existing space that could be used as a Hot COOP site. • Identify whether policies exist to trigger Hot COOP site activation.
Primary Organizational Responsibilities:
Operating PSAP facilities • Evaluate whether designated staff are properly trained to seamlessly transition to an operational Hot COOP site. • Engage in the development of training and exercises needed to develop proficiency in executing failover procedures, including activation of alternate PSAP facilities. • Evaluate whether the organization or jurisdiction has sufficient personnel and equipment to staff and sustain a Hot COOP site; acquire additional support if necessary.
Finance/administrative aspects of the PSAP • Ensure that legal and policy support and fiscal resources are available and can be authorized to engage in such exercises and agreements.
Logistical support • Procure necessary equipment and furnishings based on operational requirements and the administrative/finance organization's prior approval. • Provide any logistics needed to conduct training and exercises for Hot COOP site activation. • Identify and meet security requirements for the Hot COOP site to provide access to primary databases.
Secondary Organizational Responsibilities:
9-1-1 services planning body; at the local or state level, this may be the state 9-1-1 coordinator, a 9-1-1 service authority, or other organization • Involve state 9-1-1 coordinators in any methods of implementation or measurement of implementation.

As indicated above, there is little Federal engagement and influence involved in the steps to approve, activate, and maintain Hot COOP sites.

3.4 Evaluate the Use of Amateur Radio Networks, Talk-Around Channels, and Talk Groups and Establishing an Area Command to Manage Consequences of Incidents

Amateur radio networks, talk-around channels and talk groups, and area commands were originally developed for a variety of purposes, none of which had direct application to cyber risk management. Licensed citizens most commonly used amateur radio networks for hobby and recreational purposes, but ESS agencies, particularly in the Emergency Management

community, have found that amateur radio networks can provide a reliable means to re-establish communications between authorities when other options are not possible. Talk-around channels or talk groups are used by various ESS agencies primarily for unit-to-unit communication on the same incident scene or in line of sight, where the ability to send and receive messages without the need of a repeater tower for signal re-direction and enhancement can be easily accomplished. Area command, a means of establishing a specific area of responsibility for organizing and managing response and recovery operations for an emergency incident, also works as a stop-gap measure to reduce reliance on communications systems in deploying emergency services resources. This process can be done by assigning management resources to develop a strategy and priorities for responding to incidents in the designated area, by allocating resources according to the established priorities, and by requiring in-person reporting on the completion of response operations and readiness for another assignment.

An analysis of these activities and resources led the ESS Cyber Working Group to recommend them as available measures to respond to the cyber risk posed when communications lines are lost or disrupted. These measures may also serve the ESS well as mitigations against other threats, such as natural disasters. Generally, secondary communications options should be considered so that resumption and sustainment of emergency communications can be established in situations where the primary methods become unavailable. Options such as amateur radio networks, talk-around channels, and talk groups provide that emergency communication resource in times of primary system failure.

3.4.1 Addressing Cyber Risks Using Amateur Radio Networks, Talk-Around Channels, and Talk Groups and Establishing an Area Command

Amateur radio networks, talk-around channels and talk groups, and area commands offer effective, if low tech, communications methods, and many ESS agencies may already be using them for other purposes. Regarding cyber threats, they provide a response to cyber risks posed by the loss of communications lines that serve primary communications networks:

- Amateur Radio Networks-The use of High Frequency (HF) radio networks can be an effective workaround to use when primary land mobile radio networks are unavailable. This mitigation measure may work especially well in restoring authority-to-authority communications, such as between a local Emergency Operations Center (EOC) and a state EOC or between primary and secondary PSAP facilities. There are well established amateur radio organizations that actively support the ESS; the Radio Amateur Civil Emergency Service (RACES) and Amateur Radios Emergency Service (ARES) are two examples. The benefits of leveraging amateur radio networks include:
    - HF communications works especially well in supporting long distance communications without relying on too much infrastructure, based on the characteristics of that band of spectrum.
    - The ability to serve as a reliable form of backup communications. If communications infrastructure is disabled or damaged, HF communications can provide a suitable backup and can enable agencies to restore interagency communications as well.

- Talk-Around Channels and Talk Groups-By their very nature, talk-around channels (TAC) and talk groups are designed to support unit-to-unit communications over short distances without relying on communications infrastructure. The ability of one unit to reach another is predicated not on whether a transmission signal can reach a repeater tower, but whether the terrain and power of the transmitting radio can propagate the signal far enough to reach a receiver. Land mobile radio systems used by public safety generally fall into a few common bands of spectrum, Very High Frequency (VHF) Low Band (38-40 Mega Hertz [MHz]), VHF High Band (150-170 MHz), Ultra High Frequency (UHF) (450-470 MHz), and UHF-800 (generally located between 794-810 MHz). The benefits of using TAC and talk group communications resources include:
    - Conventional radio channels in VHF and VHF transmissions can carry farther than UHF communications before they require supporting repeaters, based on the characteristics of that spectrum.
    - Trunked radio channels use talk groups (a number of channels trunked together to permit use by the most available channel, spreading demand among frequencies to minimize congestion over the air) that can be configured to operate without repeaters to accomplish this same sort of capability.
    - Both conventional and trunked TAC/talk groups offer reliable line-of-sight transmitting and receiving capabilities.
- Area Command-According to the 2008 National Incident Management System (NIMS), "Area Commands are particularly relevant to incidents that are typically not site specific, are not immediately identifiable, are geographically dispersed, and evolve over longer periods of time…"[8] Such incidents could include those caused by cyber threats that result in the loss of communications lines that disrupt primary communications capabilities. Under an Area Command operation, the responsibilities to be addressed include but are not limited to:
    - Developing broad objectives for the affected area(s)
    - Coordinating the development of individual incident objectives and strategies
    - Allocating and re-allocating resources as the established priorities change
    - Ensuring that incidents are properly managed
    - Ensuring effective communications

Responsibilities in an Area Command environment address the potential loss of communications, which could mean that communications may be reduced to using TAC or non-repeated trunk groups over-the-air or to conducting communications face-to-face between deployed resources and command staff. . Neither of these circumstances is ideal, but they represent a low-order solution to cope with lost primary communications systems until they can be restored.

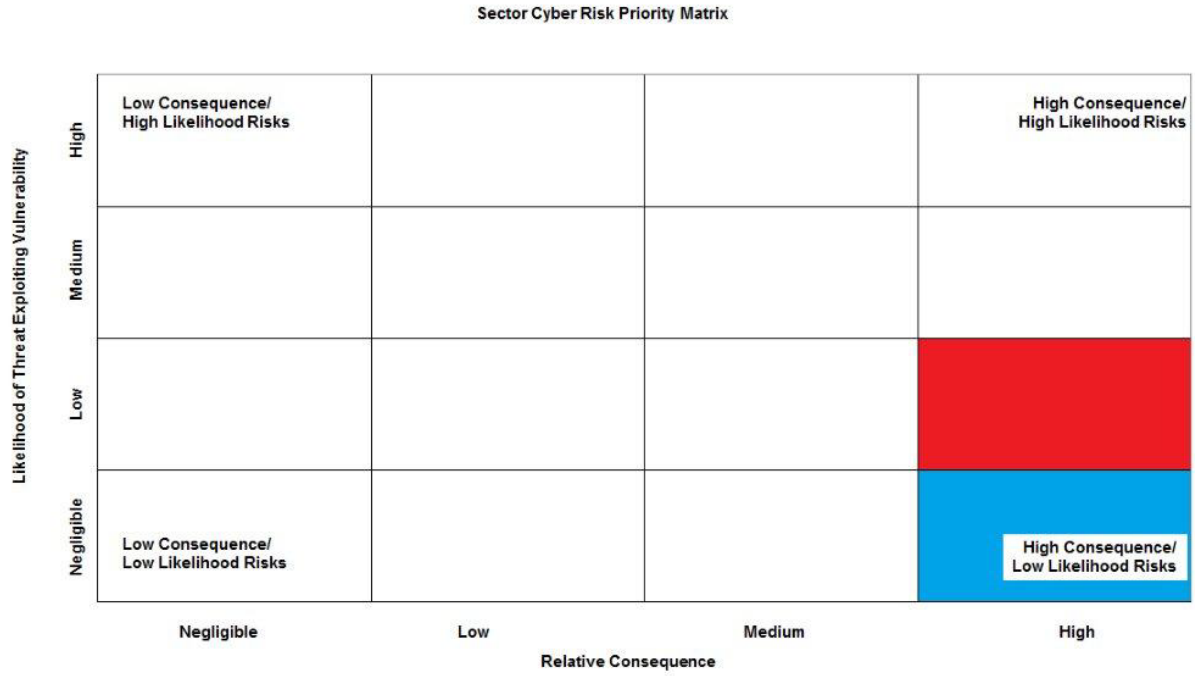
3.4.2 The Impact and Feasibility of Using Amateur Radio Networks, Talk-Around Channels, and Talk Groups and Establishing an Area Command

In the case of a deliberate attack on communications lines, most of the risk responses reduced the attack's consequences but had little effect on reducing the likelihood that

[8] "National Incident Management System," (Washington, D.C.: Department of Homeland Security, 2008).

communications lines' vulnerabilities would be exploited. Amateur radio networks, TAC and talk groups, and establishing an area command all did little to protect communications lines from the threat but slightly lowered the consequences of an incident, as indicated in Figure 15 below.

Figure 15. Estimated Level of Cyber Risk from the Loss of Communications Lines, as Depicted by the Red Block. Cyber risk analysis indicates, via the blue block, that a small reduction of cyber threats exploiting the vulnerabilities of a communications line could be achieved as a mitigation measure against intentional acts using amateur radio networks, talk-around channels and talk groups, and Area Command as a risk mitigation measure.



These cyber risk mitigation measures have already proven feasible and have made a significant impact in the sector. ARES and RACES organizations partner with ESS agencies around the country at all levels of government to use amateur radio networks to support the delivery of emergency services. TAC/Talk group resources are used on a daily basis to support radio traffic on incident scenes that may otherwise not reach repeaters, such as interior firefighters reporting on fire attack progress in a multiple-occupancy building. Area command is widely used to address circumstances such as public health emergencies, earthquakes, tornadoes, civil disturbances, and operations in a geographic area where several incident management teams are in place, and these teams are all requesting similar resources.

3.4.3 Organizational Responsibilities for Using Amateur Radio Networks, Talk-Around Channels, and Talk Groups and Establishing an Area Command

The organizational responsibility for acquiring these cyber risk mitigation measures will vary by ESS agency and jurisdiction. Arranging agreements to use amateur radio networks and qualified operators who have been vetted and approved will likely be handled by an emergency management agency director or designee. Programming radios to permit the use

of TAC/Talk Group resources will be overseen by a radio system manager. The senior ranking agency leader on duty at the time will establish an Area Command, which then must be coordinated with counterparts in other agencies of the affected jurisdiction when efforts evolve into a unified command structure. . Responsibility for implementing these cyber risk reduction measures most often lies with the key authority or group that oversees a given ESS agencies' response operations during a given period of time. This is usually an on-duty or on-call senior official, such as a chief officer, watch officer, staff duty officer, or equivalent. Table 11 below depicts how such a key authority or group could delegate responsibilities for using amateur radio networks, TAC/talk groups, or Area Command to address the loss of a communications line.

Table 11. Using Amateur Radio Networks, Talk-Around Channels, and Talk Groups and Establishing an Area Command.

Using Amateur Radio Networks, Talk-Around Channels and Talk Groups, and Establishing an Area Command
Key authority or group:
Emergency management agency, on-duty senior ranking official, on-call senior ranking official • Arrange agreements with amateur radio network organizations and vet radio operators that could be called upon to serve. • Collaborate with radio system manager and other agencies in the affected jurisdiction to assess needs and available TAC/talk group resources.
Primary Organizational Responsibilities:
On-call or on-duty senior ranking ESS agency's operations official • Order the activation of amateur radio network operators and TAC/talk group resources as needed. • Establish an Area Command structure in the area affected by the lost communications capability.
Secondary Organizational Responsibilities:
Radio system manager or communications service providing logistical support • Program radios with TAC or talk group resources to permit unit-to-unit direct communications. • Provide any logistics needed to enable amateur radio network operators with access to key ESS agency command centers and command posts.

As indicated above, there is little Federal engagement or influence in using amateur radio networks, TAC/talk groups, or Area Command to address the loss of a communications line. This is largely an agency-specific risk mitigation measure. NIMS can provide valuable insights into establishing and operating an Area Command structure to address this cyber threat.

4 USING AND ENSURING PUBLIC ALERTING AND WARNING SYSTEMS

Public alerting and warning systems can be used to provide guidance to the public in the event of a cyber threat or cyber incident when other traditional means of public contact may not be available. Yet these systems also require mitigation measures to reduce cyber risks they may encounter as well. This segment discusses the use of public alerting and warning systems for cyber threats and incidents and the steps that can be taken to ensure that messages disseminated using such systems can be relied upon.

4.1 Implement Public Alerting and Warning Systems to Provide Guidance for the Public

Overloaded communications networks can occur from a malicious actor launching a denial of service attack or from a sudden and unexpected surge in public use. Public alerting and warning systems allow emergency service personnel to communicate in a mass alert manner. Emergency personnel are able to notify and inform a greater amount of citizens in less time with public alerting systems through such means as text, email, television, and radio.

4.1.1 Addressing Cyber Risks through Public Alerting and Warning Systems to Provide Guidance for the Public

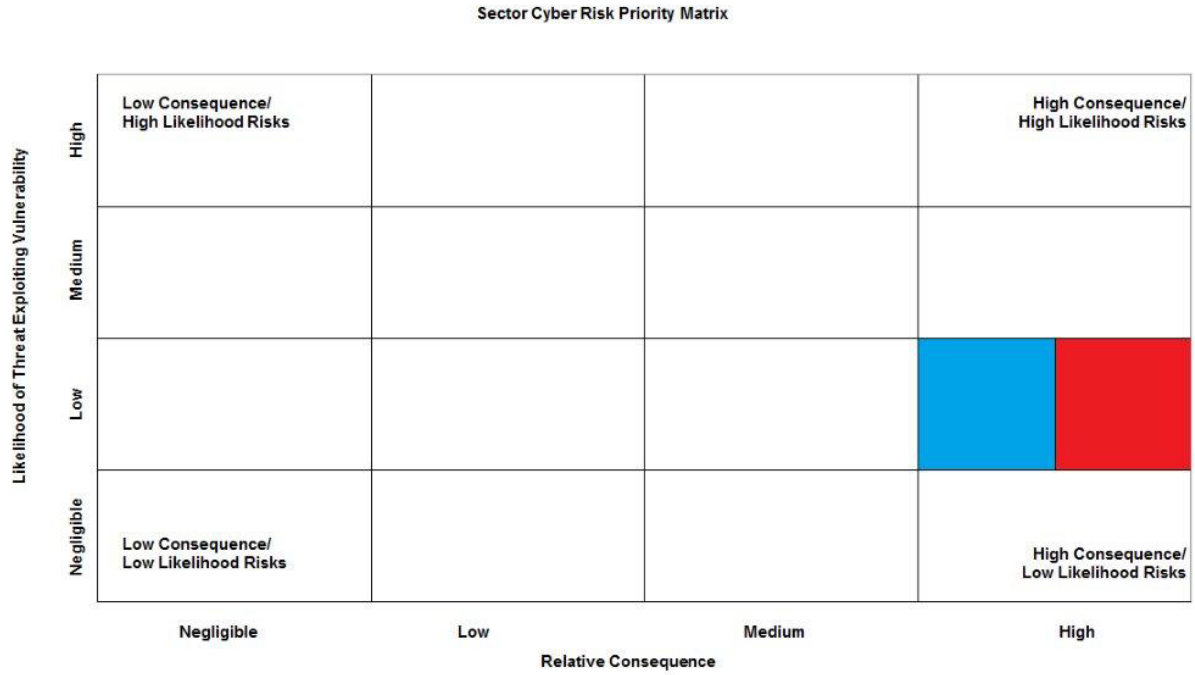
The ESS Cyber Working Group suggests that through the use of public alerting and warning systems, emergency personnel could reduce the overall consequences associated with a network overload by providing necessary guidance to the public. In the *ESS CRA*, one of the scenarios evaluated manmade deliberate and unintentional threats that could result in the loss or degradation of 9-1-1 and other emergency communications. Loss of communications could also result in the inability to deploy resources, the loss of public confidence in emergency services, and confusion or panic. This risk response can help mitigate similar incidents seen in the scenario through its use of mass communication to the public, although the mitigation may not prevent uninterrupted access during this loss of network service.

4.1.2 The Impact and Feasibility of Using Public Alerting and Warning Systems to Provide Guidance for the Public as a Cyber Risk Reduction Measure

As shown in Figure 17 on the following page, the scenario without mitigation efforts has a high likelihood of consequence. As these are reactive rather than prevention mechanisms, using public alerting and warning systems to provide guidance to the public will have no effect on the likelihood of vulnerability exploitation. The mitigation will, however, slightly reduce the consequence of exploitation—particularly as it applies to public confidence should emergency communication networks be lost or overloaded.

Evaluation of this risk response shows that implementation is highly feasibility, largely due to its low financial, political, and organizational cost. The timeframe for implementation is relatively short for this response and based on previous examples could be completed within 9–12 months.

Figure 16. Estimated Level of Cyber Risk to Overloaded Communications Network, as Depicted by the Red Block. Cyber risk analysis indicates, via the blue block, that the reduction of cyber risk that could be realized if the use of public alerting and warning systems to provide guidance to the public were deployed as a mitigation measure against cyber threats.



4.1.3 Organizational Responsibilities for Using Public Alerting and Warning Systems to Provide Guidance for the Public

Emergency managers and service personnel can best address the use of public alerting and warning system capabilities through communication and organizational teamwork with regional and local partners and systems. Responsibility for this response may reside with a combination of emergency managers, public safety communication, and/or public information officers due to the critical public information messaging component accompanying this cyber risk mitigation measure. ESS agencies should assess the capabilities of existing emergency notification systems and should work with key partners who can relay necessary communications (i.e., through TV, newspaper, radio, or social media). Additional actions that should be taken to support the implementation of alternative emergency numbers and the expansion of available 9-1-1 trunk lines can be found in Table 12 on the following page.

Table 12. Cyber Risk Mitigation Using Public Alerting and Warning Systems to Provide Guidance to the Public.

Implementing the Use of Public Alerting and Warning System to Provide Guidance for the Public
Key authority or group:
Varies by jurisdiction; Emergency manager, public safety communications and/or public relations officials, city manager, and the county CIO are all possibilities • Assess current systems and identify additional capabilities, such as alerting tools or lines that may be needed. • Identify key partners needed to properly notify public: TV, newspaper, radio, social media, etc.
Primary Organizational Responsibilities:
Emergency Management Office; at the local or state level, this may be the Emergency Manager, or other organizations that include the public relations or communications messaging component • Assess public alerting and warning procedures already in use, which lines and systems are used, and vulnerabilities of each. • Discover whether current systems and lines can reach citizens in a timely manner if and when an incident were to occur.
Secondary Organizational Responsibilities:
Operating PSAP facilities • Assess current messaging and tools used to notify the public of changes to procedure. • Decide how the public will become aware of alert notifications and whether special subscriptions will be needed for these communication methods.
Finance/administrative aspects of the PSAP • Ensure that legal and policy support and fiscal resources are available and can be authorized to use these forms of public notification.
Logistical support • Procure necessary equipment and furnishings based on operational requirements and the administrative/finance organization's prior approval. • Provide logistics needed to support the activation of agreements or to conduct training and exercises on failover procedures.

As indicated above, low Federal engagement and influence is required to implement the use of public alerting and warning systems to provide guidance to the public. Specific requirements and constraints will vary by jurisdiction, but most of the progress and constraints will concentrate at the local and state levels.

4.2 Adopt and Implement Security Policies and Procedures to Protect Sector Databases and Public Alerting and Warning Systems

Sector databases and public alerting and warning systems provide essential support services to the sector's missions. Law enforcement, firefighters, and emergency service personnel rely on database information for a variety of activities, from carrying out their first responder roles to running criminal background checks. Similarly, alerting and warning systems are used by stakeholders to disseminate information to the public. Unauthorized access to or misuse of public alerting and warning systems would result in the disruption of the sector's mission capabilities or could cause public confusion and panic. Implementing security policies and procedures, such as authentication controls, standard operating procedures, and employee use policies, would govern the use and access of sector

databases and alerting and warning systems. Authentication controls would require users to validate their identity and privileges with credentials such as a password, smart card, biometrics, or a combination of credentials. Standard operating procedures would set out guidelines on how databases are accessed and how alerting and warning systems are used. Employee use policies should describe what employees are permitted to do when using sector assets.

4.2.1 Addressing Cyber Risks with Security Policies and Procedures

The *ESS CRA* suggested that implementing security policies and procedures would address a number of risks associated with unauthorized access to sector databases and alerting systems throughout the Emergency Services Sector. One scenario in the *ESS CRA* considered the risks associated with a compromised database leading to data corruption or loss of confidentiality. Were a database compromised by unauthorized access, the corresponding data corruption or loss of confidentiality would significantly impair ESS mission capabilities. Such data corruption would render important tools such as computer-aided dispatch or criminal databases unreliable. Another scenario that would be greatly affected by unauthorized access is an alerting and warning system disseminating inaccurate information. An alerting and warning system that distributed inaccurate or false communications would likely lead to public panic or a loss in confidence over the alerting and warning system. Consequently, the public may ignore future warnings in an actual emergency because of previous false or inaccurate warnings.

These scenarios were seen as situations where security policies and procedures would help reduce risk. Implementing authentication controls serves as an effective risk response to mitigate a deliberate manmade threat while standard operating procedures and employee use policies can mitigate both deliberate and unintentional manmade threats. Some key policies included:

- Managing User Privileges-A thorough audit of user privileges and access rights will reveal whether users have an appropriate level of privilege and access. Regular privilege audits are necessary to update privileges due to changes in personnel and user roles. Because the *ESS CRA* identified open access rights as a vulnerability, developing a standard policy of role-based user privileges and applying the principle of least privilege within an organization can help protect against unauthorized access.
- Employee Use Policies-Explicitly describing acceptable and unacceptable behavior and use for sector databases and alerting and warning systems will provide a baseline for employee reference. Policies governing the use and installation of software, personal mobile devices, portable storage devices, and Internet browsing can reduce the risk of unintentionally introducing malware into a sector asset or of a malicious actor gaining access.
- Strong Passwords-Passwords alone may not provide adequate security to prevent unauthorized access. However, strong passwords can reduce the threats posed by certain password-cracking methods, such as dictionary and brute force attacks. Strong passwords are long words, phrases, or character strings that contain a combination of upper-case letters, lower-case letters, numbers, and symbols. A strong password policy also requires changing passwords on a regular basis and prevents previous passwords from being reused.

- **Multi-factor Authentication**-Where appropriate and required, multi-factor authentication will enhance authentication controls. Using combination of passwords, smart cards, tokens, or biometrics can help defend against sophisticated password-cracking tools, such as rainbow tables.
- **Editorial Review**-Specifically related to public alert and warning systems, adding a layer of editorial review to outbound communications can mitigate the risk of false or inaccurate information being released. By having communications going through a level of review, inaccurate or false information is likely to be caught before reaching the public.

4.2.2 The Impact and Feasibility of Security Policies and Procedures as a Cyber Risk Reduction Measure

The implementation of authentication controls, standard operating procedures, and employee use policies would address not only the risks identified with sector databases and alerting systems but also the prevention of unauthorized access to other sensitive systems within the sector. Such controls and policies would provide a considerable barrier to unauthorized access, both deliberate and unintentional. Policies regarding authentication controls, standard operating procedures, and employee use would reduce the likelihood of threat actors exploiting system vulnerabilities.

Authentication controls for both sector databases and public alert and warning systems were considered to be highly feasible, with an implementation time of less than 12 months. Moderate financial costs may affect the feasibility and timeliness of implementing authentication controls because outside vendors may be necessary to install authentication software or to integrate incompatible systems with a single authentication credential. Also, a change in security policy may encounter moderate cultural resistance, especially if habits around authentication and access are already ingrained. In a manmade deliberate scenario, authentication controls provide an overall risk reduction from a medium consequence and low likelihood to negligible consequence and likelihood.

Defined standard operating procedures and employee use policies both address risks described in deliberate and unintentional manmade scenarios. When these risk responses are implemented, the likelihood of a threat exploiting vulnerabilities and the level of consequences both decrease. Through training and education, standard operating procedures and employee use policies can guide and regulate employee behavior, thus reducing the likelihood and consequences of both deliberate and unintentional unauthorized access. The development of standard operating procedures and employee use policies may require a moderate level of financial cost and time to implement, but they are largely feasible with a high level of anticipated organizational acceptance. Developing and implementing comprehensive standard operating procedures and employee use policies will likely take between 12 and 24 months. Figure 17 on the following page depicts the level of risk reduction that implementing authentication controls would provide in response to a manmade deliberate threat-

Figure 17. Estimated Level of Cyber Risk to Sector Databases, as Depicted by the Red Block. Cyber risk analysis indicates, via the blue block, a reduction in the likelihood of threat exploiting the vulnerability in the event of a manmade-deliberate scenario if authentication controls were implemented.

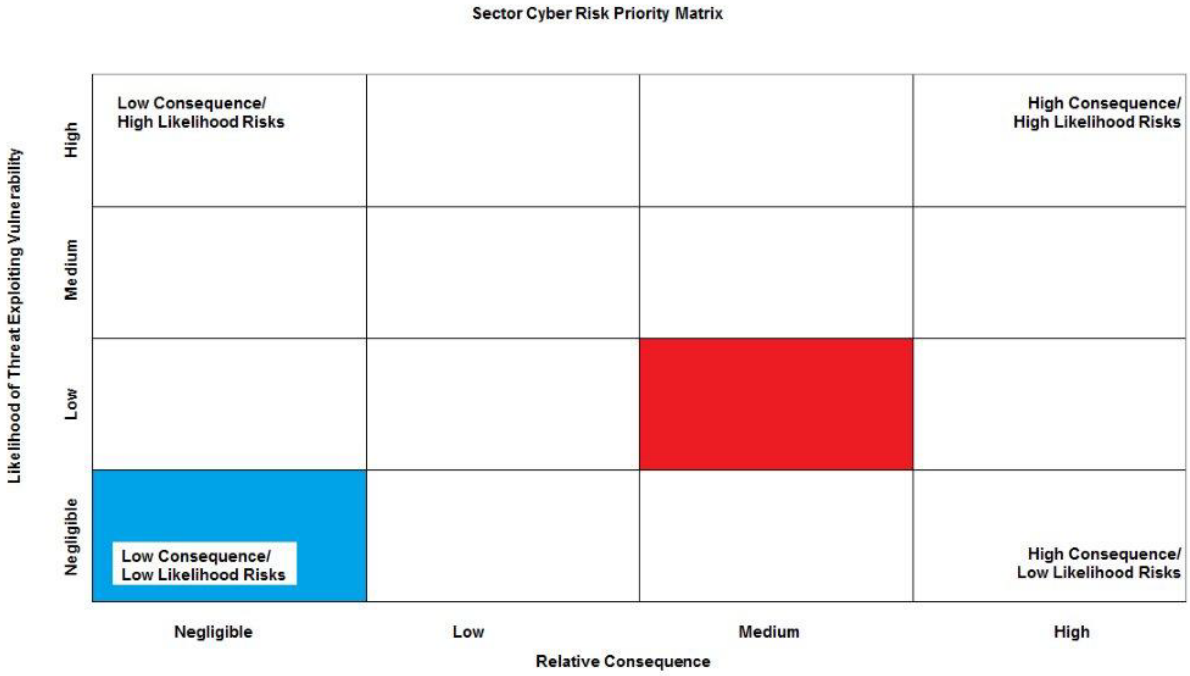
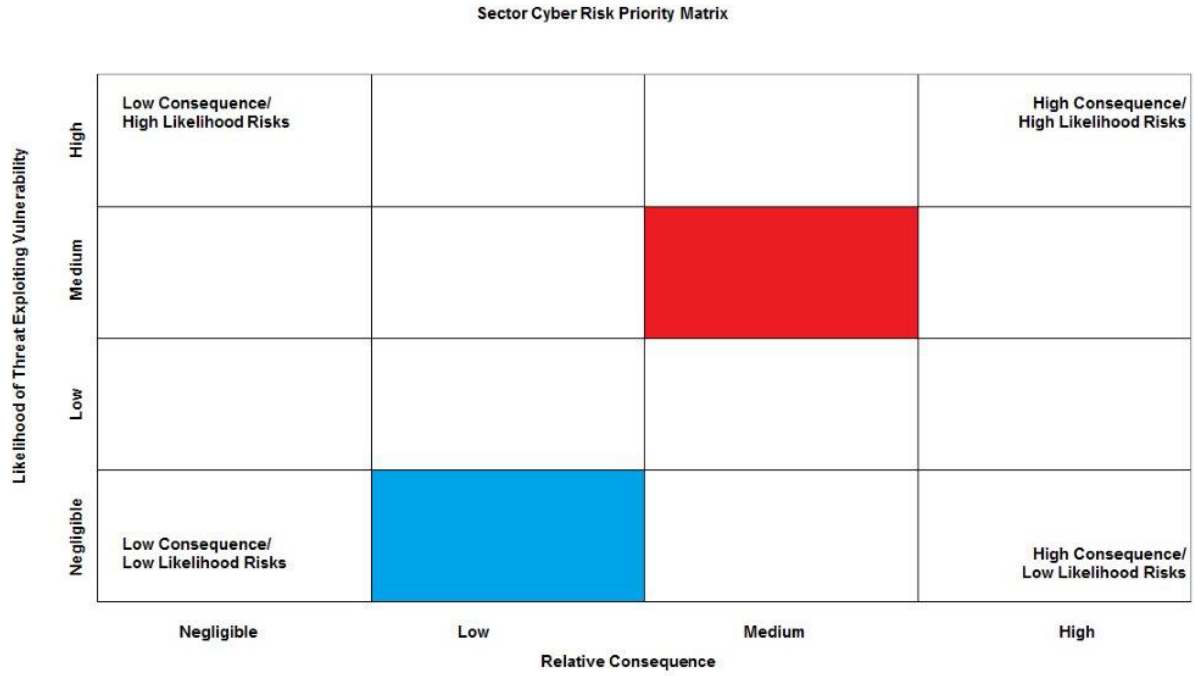


Figure 18 on the following page depicts the level of risk reduction that implementing security and employee use policies would provide in response to a manmade unintentional threat.

Figure 18. Estimated Level of Cyber Risk to Public Alerting and Warning Systems, as Depicted by the Red Block. Cyber risk analysis indicates, via the blue block, a reduction in the likelihood of threats exploiting the vulnerability in the event of a manmade-unintentional scenario if security and employee use policies were implemented.



4.2.3 Organizational Responsibilities for Implementing Security Policies and Procedures

Implementing security policies and procedures may require additional funding and effecting a cultural change within an organization. The key authorities or groups overseeing the implementation of authentication controls, standard operating procedures, and employee use policies are likely to be individual information technology (IT) managers or chief information officers at all levels of government—Federal, state, local, territorial, and tribal. Within those agencies, the leadership of the organizations using sector databases and alerting systems should assess current authentication controls, standard operating procedures, and employee use policies.

Second, leadership should determine the standards recommended by bodies such as the National Institute of Standards and Technology (NIST), or vendors can assist in recommending best practices. Then leadership should determine and develop which authentication controls, standard operating procedures, and employee use policies are most relevant and should be implemented. Table 13 on the following page depicts how such a key authority or group could delegate responsibilities for deciding how to implement security policies and procedures. Because considerable research and audits are the first steps in implementing security policies and procedures, IT managers and chief information officers at the Federal, state, local, territorial, and tribal levels of government are positioned to begin the process.

Table 13. Cyber Risk Mitigation Using Security Policies and Procedures.

Implementing Security Policies and Procedures
Key authority or group:
IT managers or chief information officers (Federal, state, local, territorial, and tribal) • Establish policy and security requirements. • Identify funding sources to finance acquisition and operation.
Primary Organizational Responsibilities:
IT managers or chief information officers; Federal, state, local, territorial, and tribal policy planners and makers • Develop policies, practices, and procedures that will implement strong security policies and procedures.
Secondary Organizational Responsibilities:
Organizations with access to operate sector databases and public alert and warning systems • Develop training and exercises needed to increase awareness of security policies and procedures among database and alerting system administrators and users.
Finance/administrative aspects of authentication controls • Ensure that technical support and financial resources are available.
Logistical support • Procure necessary software based on operational requirements and approval of the administrative or finance organization.

As indicated above, there is little Federal engagement and influence involved in the steps implementing security policies and procedures.

4.2.4 Addressing Cyber Risks with System Redundancies

The availability of cyber systems, such as communications or data transfer systems, is very important for ESS agencies to carry out their mission. If a server were to go offline or if the sole workstation responsible for broadcasting warning messages were to be compromised, the ability of sector stakeholders to respond to incidents or to complete routine tasks would be severely degraded. Consequently, mitigation against a single point of failure would address availability-related cyber risks.

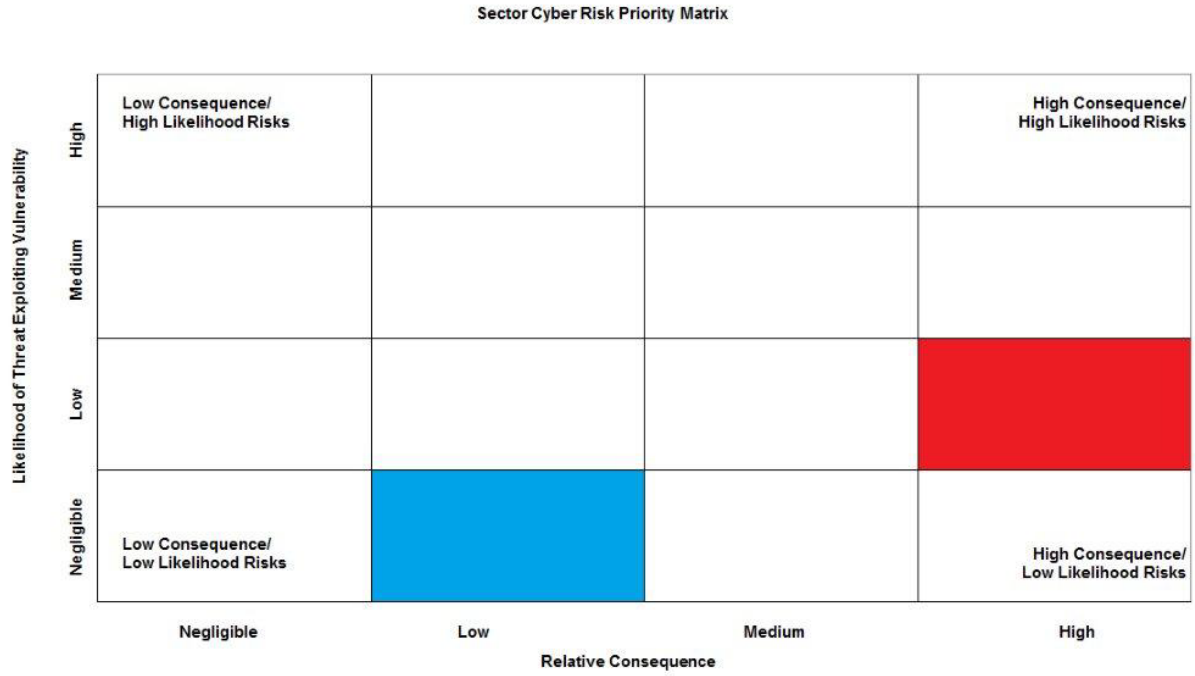
Specific to public alerting and warning systems, the *ESS CRA* identified system redundancies as a risk mitigation to prevent a malicious actor from overriding a single node within a public alerting and warning system. Without a system redundancy, a malicious actor could hijack the computer responsible for releasing emergency alert communications and thus manipulate its messages. System redundancies would force a message to go through multiple checks and approvals before a message is broadcast over the system.

4.2.5 The Impact and Feasibility of System Redundancies

System redundancies would assist in preventing a malicious actor from releasing unauthorized messages. By introducing additional layers through which a message would be required to pass, system redundancies mitigate the risk of a malicious actor taking over parts of an alerting and warning system. Such system redundancies were rated as low feasibility in terms of funding and time. The costs of acquiring and installing system redundancies are likely to be cost- and time- prohibitive, with costs unlikely to be within

reach of budgets and likely to take longer than 24 months for full implementation. Figure 19 below depicts the level of risk reduction that implementing system redundancies with security procedures and policies would provide in response to a manmade deliberate threat.

Figure 19. Estimated Level of Cyber Risk to Public Alerting and Warning Systems, as Depicted by the Red Block. Cyber risk analysis indicates, via the blue block, a reduction in the likelihood of threats exploiting the vulnerability in the event of a manmade-deliberate scenario if system redundancies were implemented along with authentication controls and editorial mechanisms.



4.2.6 Organizational Responsibilities for Implementing System Redundancies

Adopting and implementing system redundancies will require additional funding to either integrate existing systems to create the necessary redundancies or to source and purchase new technology. Table 14 on the following page depicts how a key authority can determine how to proceed with the acquisition and implementation of system redundancies. The key authorities or groups overseeing the implementation of system redundancies are likely to be individual emergency management agencies at all levels of government. Within those agencies, those responsible for public alerting and warning would need to determine the necessary level of funding and technical resources to adopt and implement system redundancies. It will then be necessary to determine which vendor and technology meets the needs of a given alerting and warning system.

Table 14. Cyber Risk Mitigation Using System Redundancies.

Implementing system redundancies
Key authority or group:
Emergency management agencies at the Federal, state, local, territorial, and tribal levels • Establish policies that require redundancy and message validation or verification prior to release. • Identify funding sources to finance the acquisition and operation of system redundancies.
Primary Organizational Responsibilities:
Emergency management agencies at the Federal, state, local, and tribal levels • Determine the technical requirements for implementing system redundancies. • Choose an appropriate vendor for installation and ongoing support.
Secondary Organizational Responsibilities:
Organizations with access to operate sector databases and public alert and warning systems • Determine the technical requirements for implementing system redundancies. • Choose an appropriate vendor for installation and ongoing support.
Finance/administrative aspects of authentication controls • Ensure that technical support and financial resources are available.
Logistical support • Procure necessary software based on operational requirements and approval of the administrative or finance organization.

As indicated in the table above, there is little Federal engagement and influence involved in the steps implementing system redundancies.

5 DEFENDING SURVEILLANCE SYSTEMS AND NETWORKS

The increasing use of surveillance systems, including Closed-Circuit Television (CCTV) systems and other technologies used to detect, prevent, deter, respond to, or recover from incidents that threaten public safety and homeland security, creates an inherent interest among those who attempting to defeat those systems. This segment address cyber risk mitigation measures to protect those systems and networks.

5.1 Implement Standards, Guidelines, and Best Practices for Surveillance Technologies and Capabilities

Surveillance technology serves as both a preventative security measure and as a necessary tool for daily operations, such as those in prison environments and those requiring positive identity before entrance. Surveillance technologies are widely used today by emergency services entities. Surveillance technology can be used not only for securing facilities from destructive attacks, but also for documenting traffic flow patterns and alerting dispatch personnel to events, such as disabled vehicles, and offer near- or real-time motor-vehicle accident discovery. Entities using surveillance systems have an assortment of expanding and upgrading surveillance technologies available. With increased use and upgrade of these technologies, the need to safeguard these components and systems is growing at the same rate.

5.1.1 Addressing Cyber Risks through Implementing Standards, Guidelines, and Best Practices for Surveillance Technologies and Capabilities

The ESS Cyber Working Group suggests that implementing standards, guidelines, and best practices for surveillance technologies and capabilities would address a number of cyber-related risks. These risks could mar the entities' ability to monitor and record potentially malicious and proactive activities affecting their facilities. This specific scenario evaluated deliberate manmade threats that could result in the loss of surveillance capabilities, criminal activity occurring without detection, tampering with evidence, and the inability to effectively control traffic or monitor public works infrastructure processes or mechanisms.

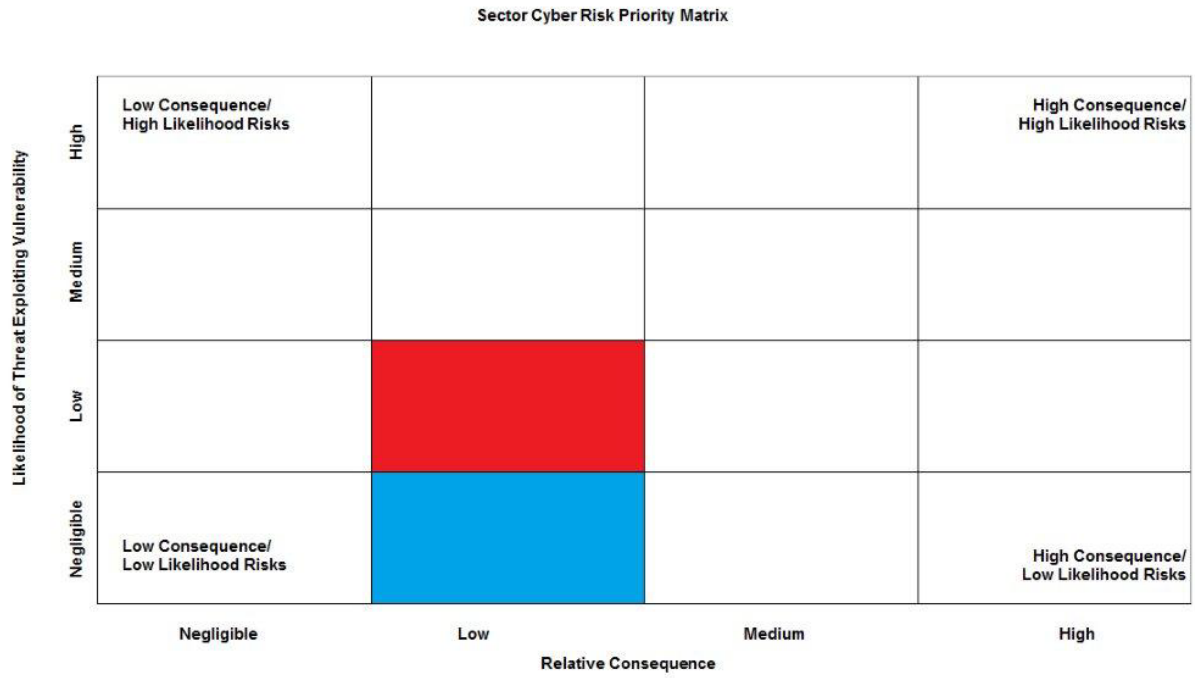
Of the risks presented, implementing standards, guidelines, and best practices was determined to be a viable mitigation in reducing deliberate manmade threats. The implementation of standards and guidelines helps provide the employee operating the surveillance systems with knowledge about the potential risks and defensive measures required to protect the system and improve its use. Drafting and implementing key mitigations like those mentioned above will help in reducing risks from insider threats.

An evaluation of employee access authorizations may be in order to understand who has access and why and at what level of authorization access they possess, such as administrator or user. The organization may discover that some employees have access and certain rights that may not be applicable to their current job duties. Disabling excessive rights to those who do not need them and applying these rights only to those who need them can be an easier mitigation to insider threat. Also, the organization should have a specific process in place for managing user rights and accesses. This will ensure that edits made now and in the future will follow the same set of guidelines creating uniformity.

5.1.2 The Impact and Feasibility of Implementing Standards, Guidelines, and Best Practices for Surveillance Technologies and Capabilities

Implementation of best practices, such as using secure connectors and developing situational awareness, will also aid the reduction of risk to the CCTV system or surveillance system attack threat. The reduction of the likelihood of threat to the vulnerability and relative consequences accomplished by this response are depicted in Figure 20 below.

Figure 20. Estimated Level of Cyber Risk to Surveillance Technology, as Depicted by the Red Block. Cyber risk analysis indicates, via the blue block, a reduction in the likelihood of threats exploiting the vulnerability in the event of a manmade-deliberate scenario. The results shown above are a projected accomplishment followed by the implementation of standards and guidelines for surveillance technologies.



Introducing and implementing best practices will moderately decrease vulnerabilities but will only slightly reduce the low rating of potential consequences. Standards, guidelines, and best practices for CCTV and surveillance systems will likely have an impact on vulnerability—lowering it from medium to low—and will only have a slight effect on consequence. The feasibility of implementing the best practices presented here can introduce cost, timing, and compatibility challenges. For example, time constraints may affect the modification or development of policies. Financial costs may increase if the agency determines that additional staff or staff hours are needed to first develop and implement these measures and then to maintain and operate them. New technology aligned with old policy can create a compatibility issue, thus requiring additional time and potential cost to align the technology with updated and applicable policy. This risk response can be completed in a reasonable timeframe, likely in less than 2 years.

5.1.3 Organizational Responsibilities for Implementing Standards, Guidelines, and Best Practices for Surveillance Technologies and Capabilities

Senior leaders, such as an agency's director or a physical or cybersecurity manager, should oversee the development of these cyber risk mitigation measures. In addition to technical knowledge about existing cybersecurity policies for the agency's CCTV or surveillance systems, there may be research needed into the laws, rules, and regulations that affect the use of CCTV and surveillance systems.

Table 15 below depicts the structure needed to successfully address and consider viable options to implementation and risk reduction.

Table 15. Cyber Risk Mitigation Using Implemented Standards, Guidelines, and Best Practices.

Implementing Standards, Guidelines, and Best Practices, for Surveillance Technologies and Capabilities
Key authority or group:
Varies by organization; organization's director or physical or cybersecurity manager • Assess leadership support for the adjustment of and addition to existing policy and guidelines. • Identify funding sources to finance acquisition and operation.
Primary Organizational Responsibilities:
Organization's planning team for surveillance standards and best practices • Research best practices and standards applicable to specific situations. • Research any applicable laws, rules, and regulations.
Secondary Organizational Responsibilities:
Organization's operating surveillance technologies and support • Develop policies, practices, and procedures that will support the implementation of surveillance technology standards. • Develop training and exercises needed to develop proficiency in the final policies.
Finance/administrative aspects of technology implementation • Ensure that legal and policy support and fiscal resources are available and can be authorized to purchase security related personnel and equipment.

As indicated above, there is little or no direct Federal influence in implementing these measures. Decisions on which mitigations to implement and/or how to implement them will be made and executed at the governmental or leadership level of the at-risk entity.

5.2 Evaluate the Physical Location of Cameras and Other Surveillance Technologies

Surveillance cameras and supporting equipment work to document and aid in the investigative process of security breaches on physical structures or other entities requiring physical protection. Surveillance equipment's visible presence can also act as a deterrent. However, working as a deterrent is not always the ideal secondary use of surveillance equipment. In some instances, potential offenders can disregard the primary role of surveillance technology and physically damage or alter the equipment if easily visible and accessible.

5.2.1 Addressing Cyber Risks through Evaluating Physical Locations of Cameras and Other Surveillance Technologies

The ESS Cyber Working Group suggests that evaluating the physical location of surveillance cameras and implementing location changes would address a number of cyber related risks

that could harm the general purpose and function of surveillance equipment. The related scenario evaluated deliberate manmade threats that could result in the loss of surveillance capabilities, criminal activity occurring without detection, tampering with evidence, and the inability to effectively control traffic or monitor public works infrastructure processes and mechanisms.

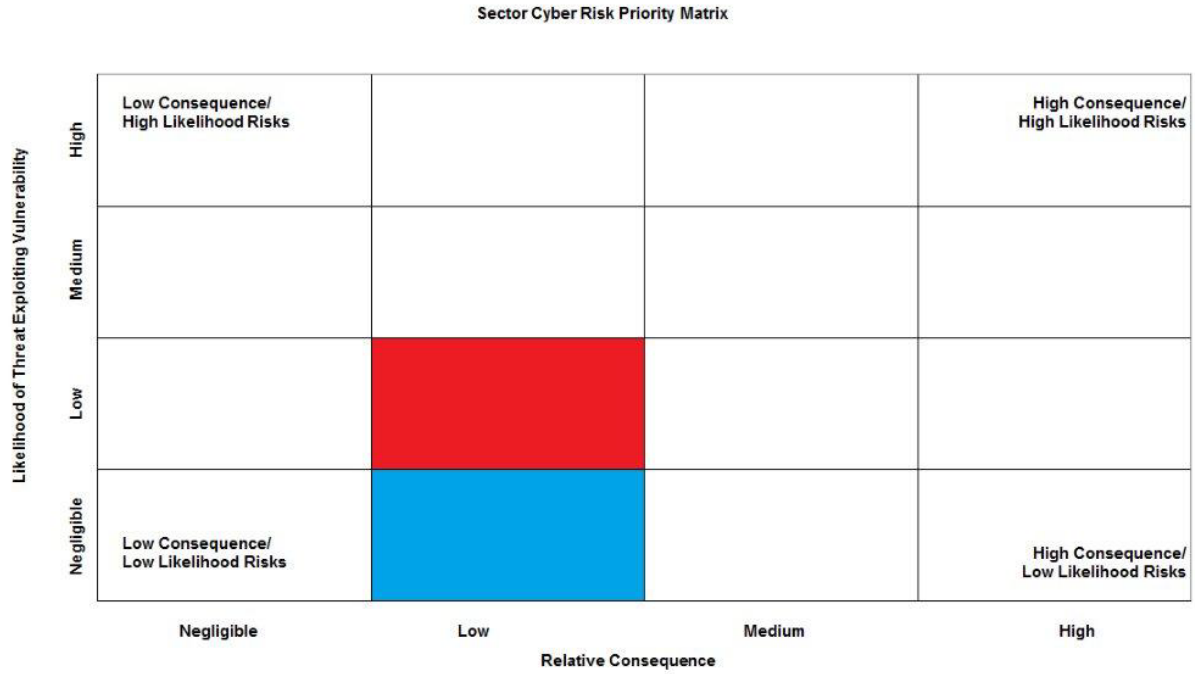
Conducting an evaluation of physical locations of cameras and other surveillance technologies served as an effective risk response to mitigating threats to CCTV and other surveillance equipment. Using camouflage techniques and relocation measures will aid in the risk reduction of physical damage done to surveillance equipment. Some possible practices that can be used are:

- **Camouflage** – Disguising the appearance of cameras and other surveillance equipment can prevent detection by criminals and thus may lower the risk of that equipment being damaged.
- **Height Adjustment** – Elevating surveillance equipment so that it is out of the reach of human capability can reduce the chances of damage done to the protected equipment.
- **Protective Enclosure** – If cameras or surveillance equipment are visible to the public for deterrent purposes, enclosing the camera in a protective housing will add to the physical security of the unit so that it can be safeguarded from damage.

5.2.2 The Impact and Feasibility of Evaluating Physical Locations of Cameras and Other Surveillance Technologies

Enhancing the physical security of cameras by strategically locating them will slightly reduce the likelihood of vulnerability exploitation but will not change potential consequences. The physical location of security cameras, such as hiding them from public view, may only reduce vulnerability to the extent that hiding cameras would make a malicious actor unaware of the target's presence. Changing the physical location of cameras represented the most feasible of risk responses. The reduction of the likelihood of threat to the vulnerability is accomplished by this response, as depicted in Figure 21 on the following page.

Figure 21. Estimated Level of Cyber Risk to Surveillance Technology, as Depicted by the Red Block. Cyber risk analysis indicates, via the blue block, a reduction in the likelihood of threats exploiting the vulnerability in the event of a manmade-deliberate scenario. The recommendation of surveillance technology physical location adjustment presented the risk reduction shown. This recommendation works generally as a preventative measure only so that only the threat of exploiting the vulnerability has been reduced.



This response was rated at a timeline level of high, indicating that the response can be completed in a relatively short timeframe (likely less than a year).

5.2.3 Organizational Responsibilities for Evaluating Physical Location of Cameras and Other Surveillance Technologies

The key authority or group overseeing the evaluation of physical location of cameras and surveillance systems will vary depending upon the organization. The key leader will likely be the organization's physical or information security manager. Table 16 on the following page depicts how such a key authority or group could delegate responsibilities for developing and implementing location changes to surveillance technology and cameras.

Table 16. Cyber Risk Mitigation Using the Evaluation of Physical Locations of Cameras and Other Surveillance Technologies.

Evaluating Physical Locations of Cameras and other Surveillance Technologies
Key authority or group:
Varies by organization; organization's physical or information security manager • Assess leadership support for adjustment to existing surveillance technologies. • Identify funding sources to finance acquisition and operation.
Primary Organizational Responsibilities:
Logistical support • Provide assistance for the implementation of new and the adjustment of existing technologies. • Procure necessary equipment and furnishings based on operational requirements and the administrative/finance organization's prior approval.
Secondary Organizational Responsibilities:
Organization's planning team for surveillance camera relocation and implementation of securing existing technologies • Develop policies, practices, and procedures that will support the implementation of new surveillance technology and the relocation of existing technology. • Map the ideal camera and supporting technology locations.
Finance/administrative aspects of technology implementation • Ensure that legal and policy support and fiscal resources are available and can be authorized to purchase security related equipment.

As indicated above, there is little or no direct Federal influence in implementing the measures presented. Decisions on which mitigations to implement and how to implement them will be made and executed at the governmental or leadership level of the at-risk entity.

5.3 Implement Artificial Intelligence to Assist with Monitoring and to Track Potential Risks

Artificial intelligence in a surveillance capability is composed of software and hardware that enable the system to recognize abnormal movements and behaviors and alert appropriate personnel. Technology exists today that allows the operating entity to store facial features and alert personnel when a system camera views a flagged person. Other examples include systems that learn a designated field of view and alert personnel when foreign objects come into view.

Artificial intelligence technology supports optimized surveillance system capabilities and provides a much greater level of security with fewer employees. One significant drawback is that artificial intelligence is a new concept, and compatibility with existing technology could be an issue. Like other types of emerging technology, however, it is likely that artificial intelligence developments will be improved upon in a short period of time. As the technology matures, it is more likely to meet the desired application needs to mitigate cyber risk.

5.3.1 Addressing Cyber Risks through Implementing Artificial Intelligence to Assist with Monitoring and Tracking Potential Risks

The ESS Cyber Working Group suggests that implementing artificial intelligence measures to surveillance systems and their supporting technology would address cyber related risks that

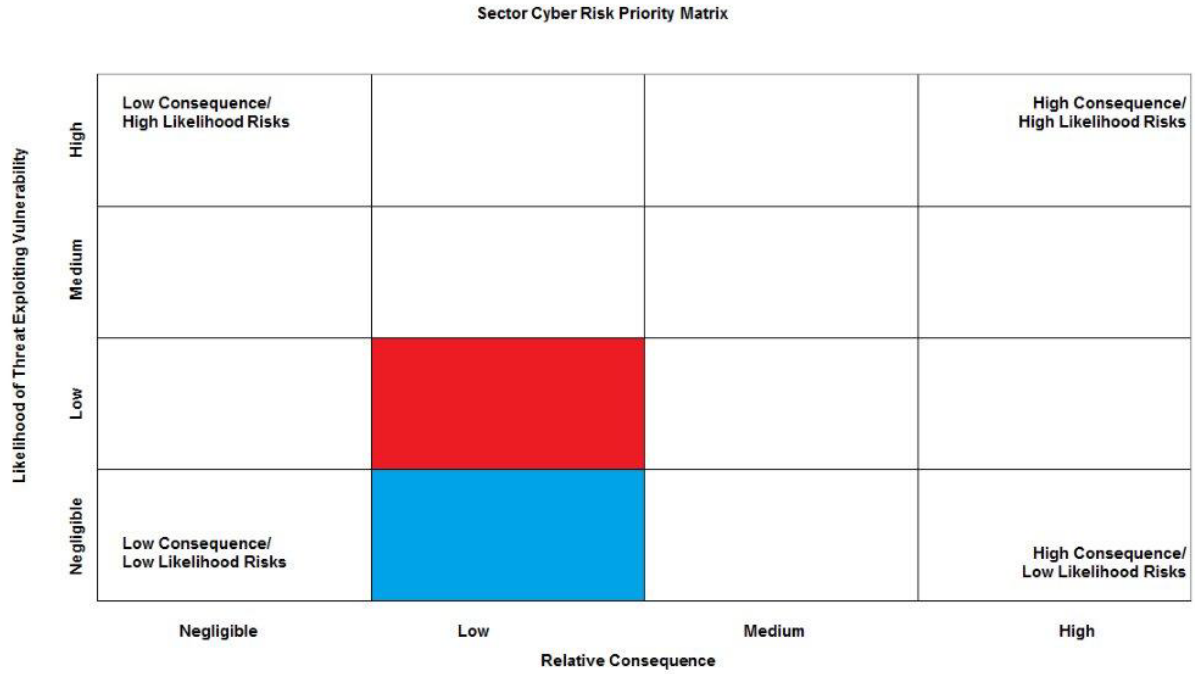
could impair the organization's ability to document and successfully use their surveillance technology. One of the cyber risk scenarios considered in the *ESS CRA* was the possibility of a deliberate manmade attack on the surveillance infrastructure. Working as a defensive measure, artificial intelligence quickly and more frequently alerts personnel of possible dangers. With less human interaction required to use the surveillance system as a whole, the personnel assigned to the task of monitoring can focus their attention on only alerts and can designate constant monitoring to the artificial intelligence. Since standards can be set and learning capabilities exist in artificial intelligence systems, the chances of human error or omissions occurring during monitoring is reduced. Allowing personnel to focus their time and energy on responding to system alerts also makes the defensive system much more effective because the new technology is less likely to miss anomalies in the monitored areas.

5.3.2 The Impact and Feasibility of Implementing Artificial Intelligence to Assist with Monitoring and Tracking Potential Risks

Using artificial intelligence for mitigation poses the risk of surveillance system damage or destruction from a deliberate manmade-attack. Evaluation of risk responses indicates that using artificial intelligence capabilities will moderately reduce vulnerability of exploitation and slightly reduce the consequences of exploitation. Artificial intelligence capabilities have the most limited feasibility of all risk responses evaluated, given costs, the length of time required to implement monitoring capabilities (estimated at 2 years or longer), and some technological and compatibility issues.

As this mitigation is a newer form of technology for most surveillance systems, the likelihood of compatibility issues exists, which may require upgraded surveillance system components or software, and the costs for this cyber risk mitigation measure may be high. The reduction of the likelihood of threat to the vulnerability is accomplished by this response, as depicted in Figure 22 on the following page.

Figure 22. Estimated Level of Cyber Risk to Surveillance Technology, as Depicted by the Red Block. Cyber risk analysis indicates, via the blue block, a reduction in the likelihood of threat exploiting the vulnerability in the event of a manmade-deliberate scenario. In the event of an attack, artificial intelligence implementation will act as a preventative measure, reducing the likelihood of the threat. The consequences of an incident were slightly reduced but not enough as to move it from low to negligible.



This cyber risk response mitigation measure is complicated to implement, given the aforementioned feasibility constraints. It can be completed as a long-term mitigation, likely over a period of 2 years or longer.

5.3.3 Organizational Responsibilities for Implementing Artificial Intelligence to Assist with Monitoring and Tracking Potential Risks

The key authority or group overseeing the implementation of artificial intelligence in a surveillance capacity will vary depending upon the organization. The key leader will likely be the organization's physical or cybersecurity manager. Table 17 on the following page depicts how such a key authority or group could delegate responsibilities for developing and implementing location changes to surveillance technology and cameras.

Table 17. Cyber Risk Mitigation through Artificial Intelligence to Assist with Monitoring and to Track Potential Risks.

Implementing Artificial Intelligence to Assist with Monitoring and Tracking Potential Risks
Key authority or group:
Varies by organization; organization's physical or information security manager • Assess leadership support for the addition of artificial intelligence technology to existing surveillance technologies. • Identify funding sources to finance acquisition and operation.
Primary Organizational Responsibilities:
Organizations planning team for artificial intelligence implementation to existing technologies • Develop policies, practices, and procedures that will support the implementation of new artificial surveillance intelligence technology. • Assess current systems and determine compatibility.
Secondary Organizational Responsibilities:
Organizations operating artificial intelligence capable surveillance systems • Develop training and exercises needed to become proficient in operating the new technology.
Logistical support • Provide assistance in implementing new and adjusting existing technologies. • Procure necessary equipment and furnishings based on operational requirements and the administrative/finance organization's prior approval.
Finance/administrative aspects of technology implementation • Ensure that legal and policy support and fiscal resources are available and can be authorized to purchase security-related personnel and equipment.

As indicated in above, there is little or no direct Federal influence involved in implementing these measures. Decisions on which mitigations to implement and how to implement them will be made and executed at the governmental or leadership level of the at-risk entity.

CONCLUSION

In support of its vision of "[a]n Emergency Services Sector in which facilities, key support systems, information and coordination systems, and personnel are protected from both ordinary operational risks and from extraordinary risks or attacks, ensuring timely, coordinated, all-hazards emergency response and public confidence in the sector," ESS has followed the CARMA framework to develop and implement its cyber risk strategy. ESS documented CARMA stages I-III in the *ESS CRA*. The *Emergency Services Sector Roadmap to Secure Voice and Data Systems* represents the fourth CARMA stage and provides ESS disciplines with actionable mitigation activities to pursue and implement in support of the sector's cyber risk strategy:

- Adopt and Implement Next Generation 9-1-1 Services
- Create and Implement Alternative Emergency Number to 9-1-1 and/or Expand the Number of Available 9-1-1 Trunk Lines
- Create Alternate Emergency Operation Centers and Additional Public Safety Answering Point Facilities
- Create Diversity in Public Safety Answering Point and Communications Infrastructure Facilities
- Implement Improved Physical Security Measures at Public Safety Answering Point and Communications Infrastructure Facilities
- Adopt and Implement Rollover Capabilities in Public Safety Answering Point and Emergency Operation Center Facilities
- Conduct and Evaluate Failover Capabilities through Exercises
- Establish Comprehensive Cybersecurity and Continuity of Operations Plan Implementation Training and Education
- Create Hot Continuity of Operations Sites with Database Backups
- Evaluate the Use of Amateur Radio Networks, Talk-around Channels, and Talk Groups and Establishing an Area Command to Manage Consequences of Incidents
- Implement the Use of Public Alerting and Warning Systems to Provide Guidance to the Public
- Adopt and Implement Security Policies and Procedures to Protect Sector Databases and Public Alerting and Warning Systems
- Implement Standards, Guidelines, and Best Practices for Surveillance Technologies and Capabilities
- Evaluate the Physical Location of Cameras and other Surveillance Technologies
- Implement Artificial Intelligence to Assist with Monitoring and Tracking Potential Risks

Although Federal resources may be available to provide insights or assistance to risk mitigation evaluation and implementation in specific ESS disciplines, addressing cyber risk is typically the responsibility for each agency to address in light of their unique mission, needs, and resources.

Consistent with its approach to date, the ESS Cyber Working Group will continue to mature its risk assessment and management approach and processes. Mitigating the risks highlighted in the ESS CRA and refining the mitigation actions identified in this Roadmap will require the continued public and private sector collaboration. Therefore, this Roadmap will continue to evolve and be revised as the sector addresses these risks and mitigations. For further information on current training opportunities or for technical assistance that may be helpful in implementing this Roadmap, contact the Emergency Services Sector Management Team at EmergencyServicesSector@cisa.dhs.gov or visit the HSIN-ES Website.