Emergency Services Sector Cyber Risk Assessment

2012

Homeland Security

Emergency Services Sector Government Coordinating Council

Memorandum of Coordination

In 2011, through the Critical Infrastructure Partnership Advisory Council framework, the Emergency Services Sector (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 (NIPP) framework, and it will inform collaborative and synchronized management of cyber risk across the sector.

The ESS-CRA is intended to provide a risk profile that ESS partners can use to enhance the security and resilience of the ESS disciplines. By increasing the awareness of risks across the public and private sector domains, the ESS-CRA serves as a foundation for ongoing national-level collaboration to enhance the security and resilience of the ESS disciplines.

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

The ESS-CRA is an 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 subject matter expertise of those participating in the sector's risk assessment activities.

The ESS-CRA is the result of a collaborative effort between ESS subject matter experts across each ESS discipline. As a result of the effort, the following activities were performed:

- Verification of sector disciplines, value chains, and associated cyber infrastructure for assessment;
- Development of seven cyber risk scenarios applied across multiple ESS disciplines;
- Identification of ESS risks from threats, vulnerabilities, and consequences within the cyber risk scenarios;
- Evaluation of threats, vulnerabilities, and consequences in ESS risks; and
- Aggregation of the risks within ESS disciplines to create an ESS risk profile.

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

- Consider ESS-CRA analysis 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-Specific Agency, as appropriate and consistent with SCC and GCC 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 SSA, in accordance with guidance provided in Homeland Security Presidential Directive - 7, as appropriate and consistent with SCC and GCC member-specific authorities, resources, and programs, to facilitate management of ESS cyber risks;
- Develop or modify existing interagency and agency-specific 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, and international entities; private sector owners, operators, 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 SCC and GCC member-specific authorities and the process described herein.

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

Signatories

W. Craig Conklin
Director,
Sector Outreach and Programs Division
Office of Infrastructure Protection
National Protection and Programs Directorate
U.S. Department of Homeland Security
Chair, Emergency Services GCC

John Thompson
Chair, Emergency Services SCC

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

Table of Contents

EXECUTIVE SUMMARY 1

1. INTRODUCTION TO EMERGENCY SERVICES SECTOR CYBER RISK ASSESSMENT 5

1.1. Risk Definition and Assessment Approach 6

1.2. Emergency Services Sector Cyber Risk Assessment Report Overview 6

2. EMERGENCY SERVICES SECTOR CYBER RISK ASSESSMENT METHODOLOGY AND PROCESS 8

2.1. Stage I: Scoping Cyber Risk Management Effort 8

2.2. Stage II: Identifying Disciplines, Value Chain, and Supporting Cyber Infrastructure 8

2.3. Stage III: Conducting a Cyber Risk Assessment 9

2.4. Stage IV: Developing a Cyber Risk Management Strategy 10

2.5. Stage V: Implementing the Strategy & Measuring Effectiveness 10

3. EMERGENCY SERVICES SECTOR DISCIPLINES, VALUE CHAINS, AND, SUPPORTING CYBER INFRASTRUCTURE 11

3.1. Law Enforcement 11

3.2. Fire and Emergency Services 12

3.3. Emergency Medical Services 14

3.4. Emergency Management 16

3.5. Public Works 17

3.6. Public Safety Communications and Coordination/Fusion 19

4. EMERGENCY SERVICES SECTOR CYBER RISK PROFILE 22

4.1. Scenario Introduction 22

4.2. Scenario 1: Natural Disaster Causes Loss of 9-1-1 Capabilities 22

4.3. Scenario 2: Lack of Availability of Sector Database Causes Disruption of Mission Capability 28

4.4. Scenario 3: Compromised Sector Database Causes Corruption or Loss of Confidentiality of Critical Information **34**

4.5. Scenario 4: Public Alerting and Warning System Disseminates Inaccurate Information **42**

4.6. Scenario 5: Loss of Communications Lines Results in Disrupted Communications Capabilities **48**

4.7. Scenario 6: Closed-Circuit Television Jamming/Blocking Results in Disrupted Surveillance Capabilities **57**

4.8. Scenario 7: Overloaded Communications Network Results in Denial of Service Conditions for Public Safety and Emergency Services Communications Networks **60**

5. EMERGENCY SERVICES SECTOR CYBER RISK ASSESSMENT KEY FINDINGS AND NEXT STEPS 67

5.1. Emergency Services Sector Cyber Risk Assessment Key Findings **67**

5.2. Next Steps **70**

APPENDIX A: EMERGENCY SERVICES SECTOR CYBER INFRASTRUCTURE AND USE IN VALUE CHAINS 71

APPENDIX B: EMERGENCY SERVICES SECTOR ACRONYM LIST 107

List of Figures

Figure 1: Cybersecurity Assessment and Risk Management Approach Stages 8
Figure 2: Emergency Services Sector Value Chain 9
Figure 3: Law Enforcement Supporting Cyber Infrastructure 12
Figure 4: Fire and Emergency Services Supporting Cyber Infrastructure 14
Figure 5: EMS Supporting Cyber Infrastructure 15
Figure 6: Emergency Management Supporting Cyber Infrastructure 17
Figure 7: Public Works Supporting Cyber Infrastructure 18
Figure 8: Public Safety Communications and Coordination/Fusion Supporting Cyber Infrastructure 21
Figure 9: Scenario 1 Consequences, Vulnerabilities, and Threats 22
Figure 10: Scenario 1—Disciplines and Cyber Infrastructure Affected 23
Figure 11: Relative Risk Profile of Scenario 1: Natural Disaster Causes Loss of 9-1-1 Capabilities 25
Figure 12: Scenario 2 Consequences, Vulnerabilities, and Threats 28
Figure 13: Scenario 2—Disciplines and Cyber Infrastructure Affected 29
Figure 14: Relative Risk Profile of Scenario 2: Lack of Availability of Sector Database Causes Disruption of Mission Capability—Manmade Deliberate 30
Figure 15: Relative Risk Profile of Scenario 2: Lack of Availability of Sector Database Causes Disruption of Mission Capability—Manmade Unintentional 31
Figure 16: Scenario 3 Consequences, Vulnerabilities, and Threats 35
Figure 17: Scenario 3—Disciplines and Cyber Infrastructure Affected 36
Figure 18: Relative Risk Profile of Scenario 3: Compromised Sector Database Causes Corruption or Loss of Confidentiality of Critical Information—Manmade Deliberate 38
Figure 19: Relative Risk Profile of Scenario 3: Compromised Sector Database Causes Corruption or Loss of Confidentiality of Critical Information—Manmade Unintentional 39
Figure 20: Scenario 4 Consequences, Vulnerabilities, and Threats 43
Figure 21: Scenario 4—Disciplines and Cyber Infrastructure Affected 44

Figure 22: Relative Risk Profile of Scenario 4: Public Alerting and Warning System Disseminates Inaccurate Information—Manmade Deliberate 45
Figure 23: Relative Risk Profile of Scenario 4: Public Alerting and Warning System Disseminates Inaccurate Information—Manmade Unintentional 46
Figure 24: Scenario 5 Consequences, Vulnerabilities, and Threats 49
Figure 25: Scenario 5—Disciplines and Cyber Infrastructure Affected 50
Figure 26: Relative Risk Profile of Scenario 5: Loss of Communications Lines Results in Disrupted Communications Capabilities—Manmade Deliberate 51
Figure 27: Relative Risk Profile of Scenario 5: Loss of Communications Lines Results in Disrupted Communications Capabilities—Manmade Unintentional 52
Figure 28: Scenario 6 Consequences, Vulnerabilities, and Threats 57
Figure 29: Scenario 6—Disciplines and Cyber Infrastructure Affected 58
Figure 30: Relative Risk Profile of Scenario 6: Closed Circuit Television Jamming/Blocking Results in Disrupted Surveillance Capabilities—Manmade Deliberate 59
Figure 31: Scenario 7 Consequences, Vulnerabilities, and Threats 61
Figure 32: Scenario 7—Disciplines and Cyber Infrastructure Affected 62
Figure 33: Relative Risk Profile of Scenario 7: Overloaded Communications Network Results in Denial of Service Conditions for Public Safety and Emergency Services Communications Networks—Manmade Deliberate 63
Figure 34: Relative Risk Profile of Scenario 7: Overloaded Communications Network Results in Denial Of Service Conditions for Public Safety and Emergency Services Communications Networks—Manmade Unintentional 64

List of Tables

Table 1: Summary of Emergency Services Sector Cyber Risk Assessment Risks and Impacts 2
Table 2: Law Enforcement Discipline 11
Table 3: Fire and Emergency Services Discipline 12
Table 4: Emergency Medical Services Discipline 14
Table 5: Emergency Management Discipline 16
Table 6: Public Works Discipline 17
Table 7: Public Safety Communications and Coordination/Fusion Discipline 19
Table 8: High-Consequence and High-Likelihood Cyber Risks to Emergency Services Sector 67

EXECUTIVE SUMMARY

The Emergency Services Sector (ESS) is a system of preparedness, response, and recovery elements that form the Nation's first line of defense for preventing and mitigating risks from manmade and natural threats. ESS is a primary "protector" for other critical infrastructure sectors. Over the past decade, ESS has become increasingly dependent on a variety of cyber-related assets, systems, and disciplines to carry out its missions. In addition to the risks presented by natural hazards—such as catastrophic weather or seismic events—ESS also faces threats from criminals, hackers, terrorists, and nation-states,[1] all of whom have demonstrated varying degrees of capability and intention to attack ESS disciplines.

Although existing security and response capabilities mitigate some threats, ESS still faces sector-wide risks to its ability to operate during emergencies. With the sector's increasing dependence on cyber technology and the continuously evolving threat landscape, assessing vulnerabilities and estimating consequences is difficult. Therefore, these issues must be dealt with in a collaborative and flexible framework that enables the public and private sectors to enhance the resilience and security of the ESS disciplines.

The Emergency Services Sector Cyber Risk Assessment (ESS-CRA) evaluates risk to the sector by focusing on the ESS disciplines. The ESS-CRA uses the Department of Homeland Security (DHS) National Cyber Security Division's (NCSD) Cybersecurity Assessment and Risk Management Approach (CARMA). The six ESS disciplines assessed in this document are Law Enforcement, Fire and Emergency Services, Emergency Medical Services, Emergency Management, Public Works, and Public Safety Communications, and Coordination/Fusion. The assessment approach is not intended to be guidance for individual entities' risk management activities. Instead, the ESS-CRA is intended to provide an all-hazards risk profile that ESS partners can use to inform resource allocation for research and development and other protective program measures to enhance the security and resilience of the ESS disciplines. By increasing the awareness of risks across the public and private sector domains, the ESS-CRA serves as a foundation for ongoing national-level collaboration to enhance the security and resilience of the ESS disciplines.

The six ESS disciplines assessed in this document are—

- Law Enforcement
- Fire and Emergency Services
- Emergency Medical Services
- Emergency Management
- Public Works
- Public Safety Communications and Coordination/Fusion

ESS Disciplines

The ESS-CRA is an initial effort to assess ESS risks across all six 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 on the knowledge and subject matter expertise of those participating in the sector's risk assessment activities. This assessment does not address all threat scenarios faced by ESS entities or their users and customers. As noted in the assessment, there are areas that require additional collaborative study and further review.

[1] A state that self-identifies as deriving its political legitimacy from serving as a sovereign entity for a nation as a sovereign territorial unit. (http://dictionary.reference.com/browse/nation%20state. Accessed on 2/7/2012)

The ESS-CRA was launched in July 2011 and continued through November 2011. During seven risk elicitation and analysis sessions, ESS subject matter experts (SMEs) performed the following:

- Verified Sector disciplines, value chains, and associated cyber infrastructure for assessment
- Developed seven cyber risk scenarios applied across multiple ESS disciplines
- Identified risks from threats, vulnerabilities, and consequences within the cyber risk scenarios
- Evaluated the threats, vulnerabilities, and consequences in ESS risks using CARMA
- Aggregated the risks within ESS disciplines to create an ESS risk profile.

Table 1 includes high-consequence and high-likelihood cyber risks for each discipline, as well as potential operational impacts.

Table 1: Summary of Emergency Services Sector Cyber Risk Assessment Risks and Impacts

Law Enforcement	
Risk	*Operational Impacts*
Natural disaster causes loss of 9-1-1 capabilities	• Unavailability of certain critical systems; possible inability to coordinate incident response or stay notified of incidents • Reduced response coordination effectiveness
Loss of communications lines as a result of an unintentional or deliberate threat results in disrupted communications capabilities	• Loss or degradation of 9-1-1 services • Compromised responder safety
Public alerting and warning system disseminates inaccurate information as a result of an unintentional or deliberate threat	• Redirection of first responders to false alarms/ wasting resources • Public confusion and panic
Fire and Emergency Services	
Risk	*Operational Impacts*
Natural disaster causes loss of 9-1-1 capabilities	• Unavailability of certain critical systems; possible inability to coordinate incident response or stay notified of incidents • Reduced effectiveness of element coordination
Loss of communications lines as a result of an unintentional or deliberate threat results in disrupted communications capabilities	• Loss or degradation of land mobile radio (LMR) communications • Ineffectiveness or redirection of response operations
Overloaded communications network as a result of an unintentional threat results in denial of service conditions for public safety and emergency services communications networks	• Inability of the general public to access emergency services • Inability to effectively deploy resources

Emergency Medical Services	
Risk	*Operational Impacts*
Lack of availability of sector database as a result of an unintentional threat causes disruption of mission capability	• Public Safety Answering Point (PSAP) system failure (misdirected or no dispatches) • Inability to access subject matter affecting emergency response procedures
Compromised sector database as a result of an unintentional threat causes corruption of critical information	• Slowed overall response time • Inability of internal staff to trust integrity of data, putting all entries in doubt
Public alerting and warning system disseminates inaccurate information as a result of an unintentional threat	• Redirection of first responders to false alarms/wasting of resources • Public confusion and panic
Emergency Management	
Risk	*Operational Impacts*
Public alerting and warning system disseminates inaccurate information as a result of an unintentional or deliberate threat	• Redirection of first responders to false alarms/wasting of resources • Action by the public that is inaccurate/ unwarranted, creating distrust and reducing effectiveness of operations
Loss of communications lines as a result of a deliberate threat results in disrupted communications capabilities	• Loss or degradation of 9-1-1 services • Ineffectiveness or redirection of response operations
Overloaded communications network as a result of an unintentional threat results in denial of service conditions for public safety and emergency services communications networks	• Inability of the general public to access emergency services • Loss of confidence in emergency services
Public Works	
Risk	*Operational Impacts*
Compromised sector database as a result of an unintentional threat causes corruption of critical information	• Loss of service, including electrical, water, wastewater • Slowed overall response time
Loss of communications lines as a result of an unintentional or deliberate threat results in disrupted communications capabilities	• Loss or degradation of 9-1-1 services • Ineffectiveness or redirection of response operations
Closed-circuit television (CCTV) jamming/blocking as a result of a deliberate threat causes disrupted surveillance capabilities	• Inability to monitor/respond to physical incident • Failure to record evidence/criminal acts

Public Safety Communications and Coordination/Fusion	
Risk	*Operational Impacts*
Natural disaster causes loss of 9-1-1 capabilities	• Unavailability of certain critical systems; possible inability to coordinate incident response or stay notified of incidents • Reduced effectiveness of element coordination
Lack of availability of sector database as a result of an unintentional or deliberate threat causes disruption of mission capability	• PSAP system failure • Redirection of resources leading to slow response and unavailability of some systems
Loss of communications lines as a result of an unintentional threat results in disrupted communications capabilities	• Loss or degradation of 9-1-1 services • Ineffectiveness or redirection of response operations

Although access to new cyber technology has enabled ESS to expand and improve its operational ability across disciplines, concern has grown regarding threats to and vulnerabilities in ESS cyber infrastructure. The results of the ESS-CRA show that cyber threats can have a significant impact on the ability of the ESS disciplines to operate. It is important for ESS stakeholders, such as cyber infrastructure owners, acquirers, managers, policy makers, and operators, to remain aware of current and upcoming cyber threats and focus on implementing security before rather than after an incident.

Although this assessment addresses several strategic risks to the ESS infrastructure that are of national concern based on the knowledge and subject matter expertise of those participating in the sector's risk assessment activities, this assessment does not address all risk scenarios faced by ESS entities or their users and customers. Still other cyber threat areas require additional collaborative study and further review by ESS stakeholders. The next step in CARMA after the ESS-CRA is to determine how risks should be addressed. ESS will continue to mature its risk assessment and management approach and processes. Addressing the risks highlighted in this assessment will require the continued public and private sector collaboration that has facilitated development of this assessment. ESS will develop and release the *Emergency Services Sector Cybersecurity Roadmap* to address risks identified in the ESS-CRA. This roadmap will describe the ESS cybersecurity risk management strategy.

1. INTRODUCTION TO EMERGENCY SERVICES SECTOR CYBER RISK ASSESSMENT

The Emergency Services Sector (ESS) is one of 18 critical infrastructure sectors identified in the National Infrastructure Protection Plan (NIPP). ESS is a system of preparedness, response, and recovery elements that form the Nation's first line of defense for preventing and mitigating the risk from manmade and natural threats. The sector consists of emergency services facilities and their associated systems, trained and tested personnel, detailed plans and procedures, redundant systems, and mutual-aid agreements that provide life safety and security services across the Nation through a first-responder community composed of Federal, State, local, tribal, territorial, and private sector partners. ESS is a primary "protector" for other critical infrastructure sectors. The loss or incapacitation of ESS capabilities would notably affect the Nation's security, public safety, and morale.[2]

Over the past decade, ESS has become increasingly dependent on a variety of cyber-related assets, systems, and functions to carry out its missions. These assets include, but are not limited to: databases, communications equipment, control systems, navigation systems, management systems, and security systems. The confidentiality, integrity, and availability of these systems are critical to ESS's ability to effectively perform its various public safety missions.

Using the Department of Homeland Security (DHS) National Cyber Security Division's (NCSD) Cybersecurity Assessment and Risk Management Approach (CARMA), ESS conducted the Emergency Services Sector Cyber Risk Assessment (ESS-CRA) to support the sector's risk management goals. Using NCSD's approach, ESS public and private sector partners collaborated to identify cyber-related risks and enhance the resilience of ESS disciplines (or critical functions) and their supporting cyber infrastructure. The ESS-CRA provides an all-hazards risk profile of the sector's cyber infrastructure, informs resource allocation for protection and management of ESS' inherent risks, and increases awareness of cyber risks across all levels of the public and private sectors. This assessment is not intended to conflict with individual entities' risk management activities or risk assessment tools such as the Emergency Services Self-Assessment Tool).

Critical Functions are sets of processes that produce, provide, and maintain a sector's products and services. For this assessment, the term *critical function* is synonymous with ESS discipline. The six ESS disciplines are—

- Law Enforcement
- Fire and Emergency Service
- Emergency Medical Services
- Emergency Management
- Public Works
- Public Safety Communications and Coordination/Fusion

With the exception of the Public Safety Communications and Coordination/Fusion function, each discipline is defined in the Emergency Services Sector Sector-Specific Plan.

ESS Critical Functions

This report describes the results of the ESS-CRA. The ESS-CRA accounts for the varying elements of ESS infrastructure, such as the human, physical, and cyber aspects. The result of the ESS-CRA is an ESS Risk Profile that identifies the ESS-wide cyber infrastructure risks and will inform and shape the sector's strategy for managing cyber risks, as well as illustrate how these risks affect the Nation. The ESS Risk Profile

[2] Emergency Services Sector-Specific Plan (2010), http://www.dhs.gov/xlibrary/assets/nipp-ssp-emergency-services.pdf). Accessed on 1/12/2012

facilitates an understanding of national-level cyber risks to ESS that stakeholders, such as cyber infrastructure owners, managers, policy makers, and operators, can leverage to make informed decisions on how to address current and potential threats to their cyber infrastructure. The ESS-CRA and its subsequent risk management strategy also fulfill key elements of NIPP and ESS Sector-Specific Plan implementation.

1.1. Risk Definition and Assessment Approach

Components of risk identified in the ESS-CRA consist of threats, vulnerabilities, and consequences. The ESS-CRA uses the DHS Risk Lexicon to define these components[3]:

- **Threat**—natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property
- **Vulnerability**—physical feature or operational attribute that renders an entity, asset, system, network, or geographic area open to exploitation or susceptible to a given hazard
- **Consequence**—effect of an event, incident, or occurrence.

The ESS-CRA defines threats as posed by manmade acts (deliberate and unintentional) or natural events. The nature of a threat can vary widely based on whether it was posed by a manmade deliberate, manmade unintentional or natural threat. The ESS-CRA analyzes each type of threat using an approach that addresses the unique attributes of these threat types.

Vulnerabilities are identified through cyber-related people, processes, and technology perspectives. The approaches for assessing vulnerabilities for manmade deliberate and unintentional cyber threats are similar and focus on a vulnerability's extent of exposure (e.g., how easy is it to identify the vulnerability and how long does a threat potentially have to exploit it) and how easy it is to exploit.

Consequences in the ESS-CRA are analyzed similarly for all cyber threat types (i.e., manmade deliberate, manmade unintentional, and natural). The assessment includes the impacts of consequences on the sector's disciplines or services as well as impacts that cascade to users that rely on the sector's disciplines. The consequences assessment uses the four consequence criteria derived from Homeland Security Presidential Directive - 7 [4]: National and Homeland Security, Economic, Human, and Public Confidence.

After completing the cyber threat, vulnerability, and consequence assessments, the results are used to develop risks for the ESS risk profile. Risks consist of the likelihood of a threat exploiting an identified vulnerability and the expected impact or consequence of the particular event.

1.2. Emergency Services Sector Cyber Risk Assessment Report Overview

The ESS-CRA identifies cyber risks to the ESS disciplines. The assessment was conducted within the NIPP's partnership framework, and it included subject matter experts (SME) from

[3] DHS Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf. Accessed on 12/14/2011

[4] Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection, http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm. Accessed on 12/14/2011

across the ESS disciplines. The SMEs identified the sector's cyber infrastructure, its linkages to the disciplines' key activities, scenarios that could affect the sector's cyber infrastructure, and the specific risks associated with the sector disciplines based on these scenarios.

- Section 2 of the report describes the methodology and approach used to derive the content and analysis presented in Sections 3 and 4.
- Section 3 provides context to the ESS cyber infrastructure landscape by defining the disciplines and their cyber infrastructures. Appendix A lists common ESS cyber infrastructure by discipline and outlines their roles in key Sector activities.
- Section 4 presents the ESS risk profile, which describes the relative risks across the scenarios and the ESS disciplines as well as the rationale and analysis that support the risk profile.
- Section 5 discusses ESS-CRA key findings and next steps.

To address the anticipated cross-discipline audience for the report, some of the content in Section 4 is reemphasized across more than one scenario; thereby, creating some overlap or redundancy in language. The authors of this report tried to balance the anticipated demand for cross-discipline analysis with a discipline-specific description of ESS cyber risks. In balancing these anticipated audience demands, the authors have outlined the cyber infrastructure in a discipline-specific manner while articulating cross-discipline risks in a scenario-specific manner.

2. EMERGENCY SERVICES SECTOR CYBER RISK ASSESSMENT METHODOLOGY AND PROCESS

This ESS-CRA was developed using CARMA both to define the ESS cyber risk profile and to guide the sector's cyber risk management activities. As illustrated in Figure 1, the ESS-CRA contains five distinct stages.

Stages I (Scope Risk Management Activities), II (Identify Cyber Infrastructure), and III (Conduct Cyber Risk Assessment) are captured in this assessment report. Stage IV (Develop Cyber Risk Management Strategy) will be accomplished through the ESS Roadmap to Secure Voice and Data Systems in the *Emergency Services Sector Cybersecurity Roadmap*, which will describe the strategies for addressing cyber risks to the sector. Stage V (Implement Strategy & Measure Effectiveness) will be articulated and tracked through annual reporting processes that support the NIPP and the ESS Cybersecurity Roadmap.

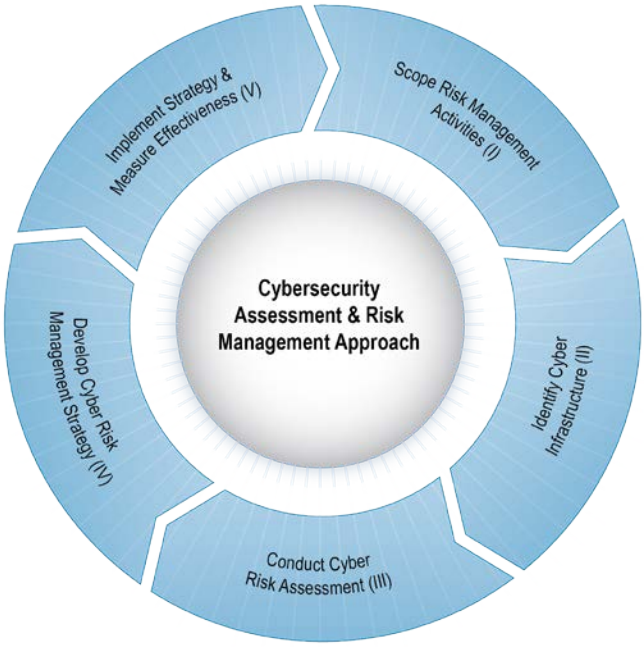

Figure 1: Cybersecurity Assessment and Risk Management Approach Stages

2.1. Stage I: Scoping Cyber Risk Management Effort

The risk assessment participants included representatives from State and local governments as well as the private sector to scope the ESS-CRA. The first activity undertaken was the establishment of the assessment team, including key leaders and ESS SMEs. Next, the ESS-CRA participants conducted the initial scoping of the assessment. During this process, the ESS-CRA participants concluded that the ESS-CRA engagement should be a sector-wide effort, rather than focusing on individual public safety disciplines, and should be used to address high profile cyber threats. With initial scoping complete, the participants began the process of defining and developing a draft set of disciplines for the ESS-CRA.

2.2. Stage II: Identifying Disciplines, Value Chain, and Supporting Cyber Infrastructure

After completing Stage I, the ESS-CRA participants collectively finalized a list of six disciplines. The six ESS disciplines included those defined in the ESS SSP plus one additional discipline, Public Safety Communication and Coordination/Fusion, which focused on an emerging activity in the community. The specific disciplines evaluated in the assessment are—

- Law Enforcement
- Fire and Emergency Services
- Emergency Medical Services

- Emergency Management
- Public Works
- Public Safety Communication and Coordination/Fusion (PSC&C)

The next step was the development of a common value chain shared by each of the six ESS disciplines. The value chain in Figure 2 represents a set of processes ordered in a typical life cycle that supports each of the ESS disciplines. The six disciplines include capabilities in each element of the value chain.

Figure 2: Emergency Services Sector Value Chain

After the development of the value chain, SMEs identified the types of cyber infrastructure supporting each of the six ESS disciplines. Cyber infrastructure includes electronic information and communication systems, and the information contained in these systems. Computer systems, control systems such as Supervisory Control and Data Acquisition systems, and networks such as the Internet are all part of cyber infrastructure. Examples of ESS cyber infrastructure include: dispatching systems, criminal database systems, radio and telecommunications infrastructure and equipment, and public alert systems. A complete list of cyber infrastructure identified for the ESS-CRA is presented in Appendix A, which also describes how this infrastructure is deployed and used across the value chains of each discipline. Section 3 of this report provides details on the six ESS disciplines, their common value chain, and each discipline's supporting cyber infrastructure.

Emergency Services Sector Cyber Risk Assessment Risk Scenarios

- Natural disaster causes loss of 9-1-1 capabilities
- Compromised Sector database causes disruption of mission capability
- Compromised Sector database causes corruption of critical information
- Public alerting and warning system disseminates inaccurate information
- Loss of communications lines results in disrupted communications capabilities
- Closed-circuit television (CCTV) jamming/blocking results in disrupted surveillance capabilities
- Overloaded communications network results in denial of service conditions for public safety and emergency services communications networks

Cyber Risk Assessment Risk Scenarios

2.3. Stage III: Conducting a Cyber Risk Assessment

During Stage III, ESS SMEs developed seven risk scenarios to assist in the identification and determination of the severity and compounding effects of various cyber threats. The risk assessment approach evaluated threats to the disciplines, associated vulnerabilities, and consequences identified in scenarios; considered the effectiveness of mitigations that are already in place; and proposed new or enhanced capabilities needed to effectively manage risk. To provide comparable results among and across disciplines, SMEs provided analyses, offered

consistent ratings, and identified measurements to be used during the evaluation of threats, vulnerabilities, consequences, and mitigations. These ratings were accompanied by descriptions and were used to develop the ESS overall risk profile.

ESS-CRA participants also considered broader questions to determine the cyber incident's direct consequences for the ESS disciplines and cascading consequences that could affect other critical infrastructure sectors, such as—

- What happens if the incident occurs?
- How severe will the consequences be?
- What customers or stakeholders are likely to be affected and how?

Finally, during each of these scenarios, participants assessed the likelihood of the event occurring and the consequences of such an event using a scoring spectrum that examined the event's effect on the discipline's/disciplines' capabilities or mission effectiveness. Events that earned a "high" rating rendered end users unable to meet foundational and basic mission requirements, while events that earned a "negligible" rating allowed end users to fully complete their missions and continue operations. Section 4 of this report shows the analysis and describes the results of the ESS-CRA.

2.4. Stage IV: Developing a Cyber Risk Management Strategy

Stage IV of CARMA is the development of a risk management strategy based on the cyber risks identified and prioritized in the ESS Cyber Risk Profile. This process involves determining how much risk is reduced by various responses as well as identifying obstacles that may arise during implementation. The approach includes the consideration of tertiary benefits or unintended negative consequences that various cyber risk responses would potentially have on disciplines within the sector or infrastructure outside the sector. The result is a clear picture of how ESS cyber infrastructure stakeholders should respond to each risk. They can choose to accept the risk, take steps to avoid it, attempt to transfer the risk to other entities, or actively mitigate the risks. The Cyber Risk Profile developed through this ESS-CRA will provide input to the Roadmap to Secure Voice and Data Systems in the *Emergency Services Sector Cybersecurity Roadmap*, which will articulate a cyber risk management plan for the sector.

2.5. Stage V: Implementing the Strategy & Measuring Effectiveness

The final stage of CARMA, Stage V, is the implementation stage. The implementation of the strategy is essential in managing sector-wide risks and reducing the sector's risk according to the strategy. The risk management strategy will identify the implementing entities—whether government or private sector—and factors in managing the rollout or deployment of the strategy elements. Risk management strategy activities will also include feedback loops that periodically assess the effectiveness of each response. Finally, risk management strategy activities will contain milestones that can guide, measure, and inform future resource allocation and risk management decisions.

Together, the five CARMA stages offer a holistic and repeatable approach for managing cyber risk in environments where infrastructure is interconnected, interdependent, and critical to everyday sector operations.

3. EMERGENCY SERVICES SECTOR DISCIPLINES, VALUE CHAINS, AND, SUPPORTING CYBER INFRASTRUCTURE

This section describes each of the ESS disciplines, the common value chain they share, and the cyber infrastructure that supports each discipline. While each of the six ESS disciplines is distinct, they are interdependent in their support of ESS's overall mission.

3.1. Law Enforcement

Table 2: Law Enforcement Discipline

Discipline/Discipline	Description
Law Enforcement	The purpose of this discipline is to maintain law and order and to protect the public from harm. Activities may include enforcement of traffic and criminal laws, prevention, detection, response, investigation, detention, court security, intelligence gathering and dissemination, and other associated capabilities and duties.

The Law Enforcement discipline includes law enforcement personnel and law enforcement agencies (LEA), and the assets, systems, and networks that support law enforcement personnel and LEAs. Law enforcement facilities contain the personnel, equipment, and vehicles used to protect the public, enforce the law, conduct criminal investigations, gather and protect evidence, and apprehend perpetrators of crimes.

An LEA may be established and authorized by Federal, State, local, tribal, and territorial-level laws, and are typically government organizations charged with serving the jurisdictions they are sworn to protect and contributing to the public safety and quality of life by maintaining law and order. This responsibility encompasses a broad range of activities associated with the authority to enforce the criminal, traffic, and in some cases, civil laws that protect their jurisdictions. Law enforcement officers are responsible for preventing, detecting, and investigating criminal acts and apprehending and detaining individuals suspected and/or convicted of criminal offenses.

Law enforcement consists of a variety of personnel, such as constables, police officers, sheriffs, deputies, State troopers, State patrols, and State police. It also includes criminal investigators, game wardens, park rangers, Special Weapons and Tactical teams, bomb squads, motor carrier safety enforcement personnel, Federal agents, marshals, and officers. LEA personnel use a variety of cyber technology infrastructure to support their efforts and accomplish their mission.

Figure 3 provides an overview of the most common cyber infrastructure resources for the Law Enforcement discipline and illustrates where in the value chain those resources may be used. A description of the cyber infrastructure supporting the Law Enforcement discipline can be found in Appendix A.

Figure 3: Law Enforcement Supporting Cyber Infrastructure

3.2. Fire and Emergency Services

Table 3: Fire and Emergency Services Discipline

Discipline/Discipline	Description
Fire and Emergency Services	The purpose of this discipline is to prevent and protect against the loss of life or property to fire, hazardous materials (HAZMAT) releases, or other hazards, natural or technological. Activities include life safety and public education, review and approval of building plans, fire safety and HAZMAT code enforcement, fire safety inspections, fire confinement and suppression, containment of HAZMAT releases and spills, property salvage, and environmental protection. Personnel in this discipline are also often trained to deliver emergency medical care in the course of their duties. They may also be trained to conduct special operations such as confined space rescues, heavy tactical rescues, above and below grade rescues, urban searches and rescues, marine and dive rescues, and wilderness rescues.

The fire and emergency services discipline involves highly trained personnel tasked with minimizing loss of life and property during incidents that result from fire, medical emergencies, HAZMAT releases, terrorist attacks, natural and manmade disasters, and other emergencies.

Fire and emergency services personnel are trained to perform fire prevention activities such as public education, building plans review, and code enforcement. They are also trained in response operations that require skilled firefighting and rescue techniques. Many fire and emergency services personnel also have additional training and equipment to engage in wildland firefighting, emergency medical services (EMS), urban and wilderness search and rescue, HAZMAT response, marine firefighting and rescue, aircraft rescue and firefighting, or explosive ordnance disposal.

Although career firefighters protect a large portion of the population, roughly three-quarters of the firefighters in the United States are volunteers who may or may not be a part of an organization with direct ties to a government function.[5] This discipline is traditionally carried out by public sector employees, but there are a number of private sector departments (e.g., industrial fire brigades and HAZMAT response teams) or contractors (e.g., commercially operated community fire services, wildland firefighters, and aviation fire and medical evacuation services) across the country. Most volunteer fire departments are non-governmental organizations (NGO) incorporated for the purpose of protecting and serving the communities in which they are located.

Figure 4 illustrates the major types of cyber infrastructure and how they support the fire and emergency services discipline. A description of the cyber infrastructure supporting the fire and emergency services discipline can be found in Appendix A.

[5] National Fire Protection Association, http://www.nfpa.org/categoryList.asp?categoryID=955&URL=Research/Fire%20statistics/The%20U.S.%20fire%20service. Accessed on 12/12/2011

Figure 4: Fire and Emergency Services Supporting Cyber Infrastructure

3.3. Emergency Medical Services

Table 4: Emergency Medical Services Discipline

Discipline/Discipline	Description
Emergency Medical Services	The purpose of this discipline is to provide first aid, rapid intervention, treatment, and transportation of the sick and injured. Activities include skilled assessment of vital signs and symptoms, triage, treatment, and transportation using ground, marine, or aviation resources to an appropriate medical receiving facility within the first hour following the request for services. Emergency medical care may be delivered in basic life support or advanced life support tiers of service, in which the latter permits care providers to use advanced specialized training, diagnostic equipment, and controlled medications to treat acutely medically ill patients or patients suffering from traumatic injury.

EMS systems consist of emergency medical care provided at the scene of a medical or traumatic incident, during an infectious disease outbreak, and during patient transport and delivery to a hospital or other treatment facility. Responses to incidents include handling the triage, treatment, and transport of all injured and ill patients; taking appropriate steps to protect staff, patients,

facilities, and the environment; and helping to monitor response teams while providing needed comprehensive medical care and mental health support to patients and their families.

EMS system capabilities within the sector include dispatching appropriate EMS resources; providing feasible, suitable, and medically acceptable pre-hospital triage and treatment of patients; and providing transport and medical care en route to the appropriate receiving treatment facility as well as initial patient tracking. EMS systems include highly skilled emergency medical technicians and paramedics, as well as highly sophisticated emergency medical vehicles, such as air and ground ambulances, that provide equipment, supplies, and transport for injured patients. Many EMS personnel are cross-trained as firefighters, and similar to those in the Fire and Emergency Services discipline, include both career and volunteer personnel.

In the EMS discipline, the breadth of cyber infrastructure is intended to promote proper documentation of patient treatments and interventions, facilitate communication with medical control, and convey an accurate report of what happened to the patient before response, during assessment, triage, and treatment, and after interventions and transportation to provide a continuous picture of the patient's condition seamlessly from the field and into the receiving facility. EMS also coordinates financial transactions (e.g., billing). These services may not exist in a single system but can be shared among fire department, ambulatory services, hospitals, and emergency management. The types of resources used to support this effort and the value chain are depicted in Figure 5. A description of the cyber infrastructure supporting the EMS discipline can be found in Appendix A.

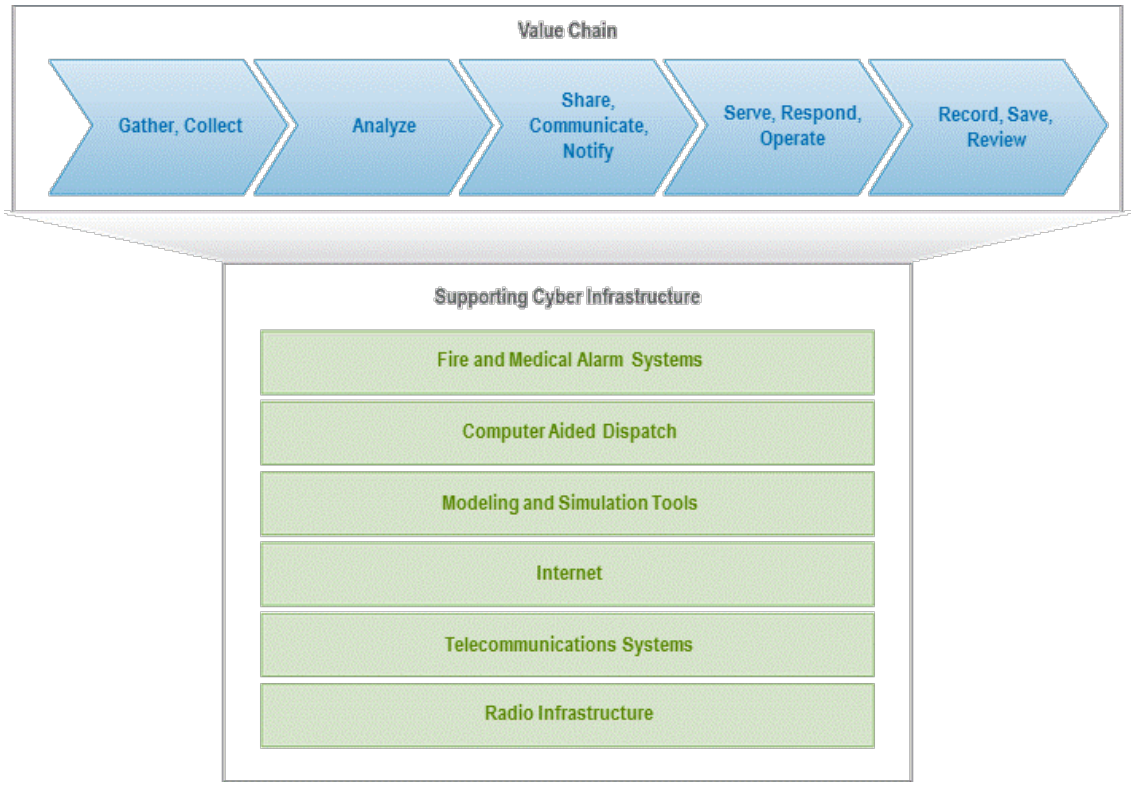

Figure 5: EMS Supporting Cyber Infrastructure

3.4. Emergency Management

Table 5: Emergency Management Discipline

Discipline/Discipline	Description
Emergency Management	The purpose of this discipline is to provide the decision support and fiscal resources needed to prevent, mitigate, respond to, and recover from natural or technological disasters. Activities include policy development, planning, strategy formation, training, and exercises to prepare government agencies and the public for major emergencies. These activities cross the pre-incident, crisis, and response phases of all disaster types.

Emergency management agencies are responsible for providing overall pre-disaster planning and other programs, such as training and exercises for natural and manmade disasters that can affect a community. Using an all-hazards approach, the emergency management discipline is carried out by a combination of partners that represent Federal, State, local, tribal, and territorial levels of government; NGOs; and private organizations and agencies.

While much of the work in mitigation, preparedness, response, and recovery preparations takes place in an office environment, the imminent threat or actual occurrence of an incident requires a more appropriate site for managing and coordinating resources and efforts. This site is typically an Emergency Operations Center (EOC), where key decisionmakers from affected agencies and jurisdictions can gather to support on-scene incident commanders, prioritize the allocation of resources, collaborate on strategy and tactics, and manage the fiscal and social consequences of an incident too complex for decision support from regular offices or a communications center, or too large for any single agency, or perhaps any single government, to manage on its own.

Emergency management agencies deliver the capability to provide multi-agency coordination for incident management by activating and operating an EOC for a pre-planned or no-notice event. EOC management includes EOC activation, notification, staffing, and de-activation; management, direction, control, and coordination of response and recovery activities; coordination of efforts among neighboring governments at each level and among local, regional, State, and National Operations Center (NOC) or command and control facilities; coordination of public information and warning; and maintenance of the information and communication necessary for coordinating response and recovery activities. Similar entities may include the National (or Regional) Response Coordination Center, Joint Field Offices, NOC, Joint Operations Center), Multi-Agency Coordination Center), and the Initial Operating Facility.

An emergency management agency identifies, in collaboration with the government agencies of the jurisdiction served, the natural and technological risks and threats that may affect the health, safety, and well-being of the jurisdiction. It develops the strategic approach for mitigating those risks, preparing to face those threats, responding to actual incidents, and recovering from them in a systematic and deliberate fashion to restore order and reconstitute essential services, residency, and commerce. The emergency management agency then develops contingency and emergency operating plans, mutual- and automatic-aid agreements, and intergovernmental agreements. They also develop elements to cover situational awareness, the common operating picture, communications, and information elements.

Emergency management agencies rely on several types of cyber technology resources to fulfill their mission and accomplish their objectives. These types are depicted in Figure 6. A description of the cyber infrastructure supporting the emergency management discipline can be found in Appendix A.

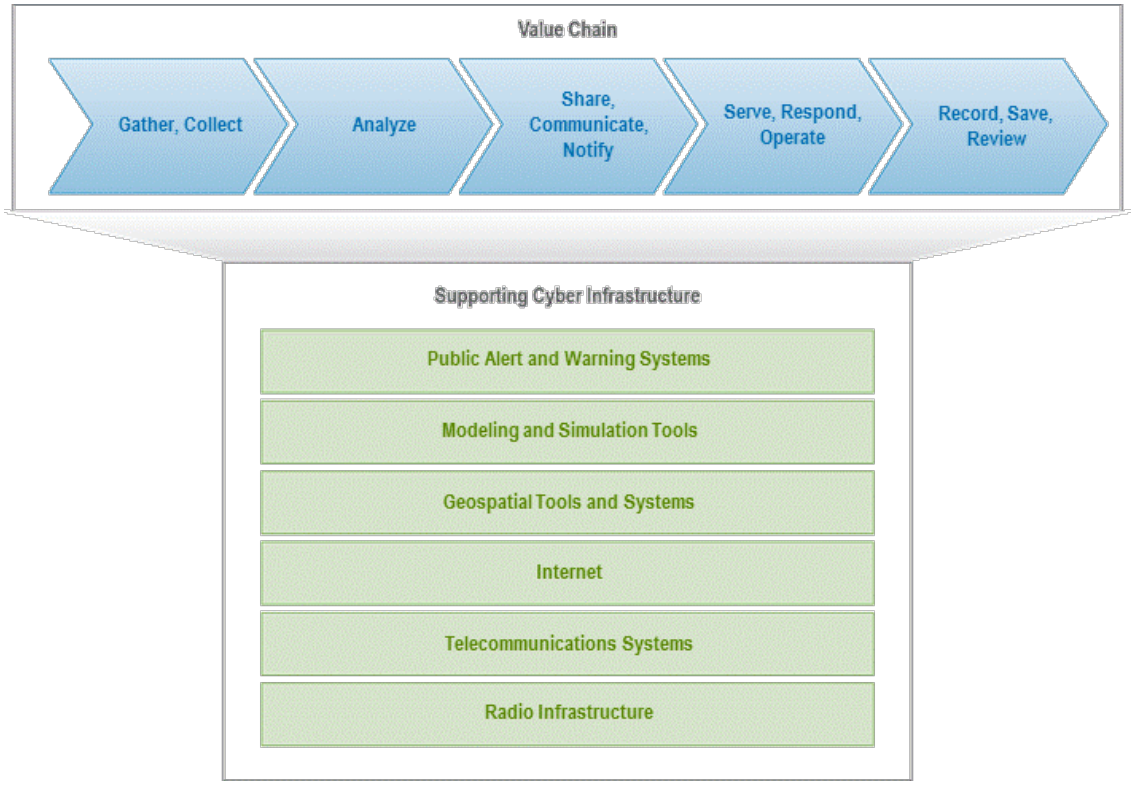

Figure 6: Emergency Management Supporting Cyber Infrastructure

3.5. Public Works

Table 6: Public Works Discipline

Discipline/Discipline	Description
Public Works	The purpose of this discipline is to provide for the design, development, and implementation of core governmental services that support transportation, utilities, communications, sanitation, domestic water supplies, and emergency response and recovery. Activities include engineering services, utility services, demolition, hazardous material response, construction of highways and walkways, erection of bridges and flood control measures, water and sewer treatment and distribution, trash and debris collection and disposal, and traffic control and signage.

Entities in the public works discipline provide essential emergency response services such as inspecting and assessing damage to buildings, roads and bridges; clearing, removing, and disposing of debris; restoring utility services; and managing emergency traffic and restoring traffic patterns. With its responsibility for making security enhancements to harden critical

facilities and monitoring the safety of public water supplies, public works is an integral component of a jurisdiction's emergency planning, prevention, response, and recovery efforts. Public works departments supply heavy machinery, raw materials, equipment operators, engineering services, and manual labor, all of which are critical to daily community maintenance and preparedness.

To supplement their own resources or to bolster those of other agencies in an emergency, public works departments often enter into mutual aid or intergovernmental agency agreements with other communities or States to provide personnel, equipment, and materials during a response and recovery effort. Public works departments may also manage contracts for additional labor, equipment, or services that may be needed during an incident.

Figure 7 depicts public works discipline cyber technology resources across the value chain. A description of the cyber infrastructure supporting the public works discipline can be found in Appendix A.

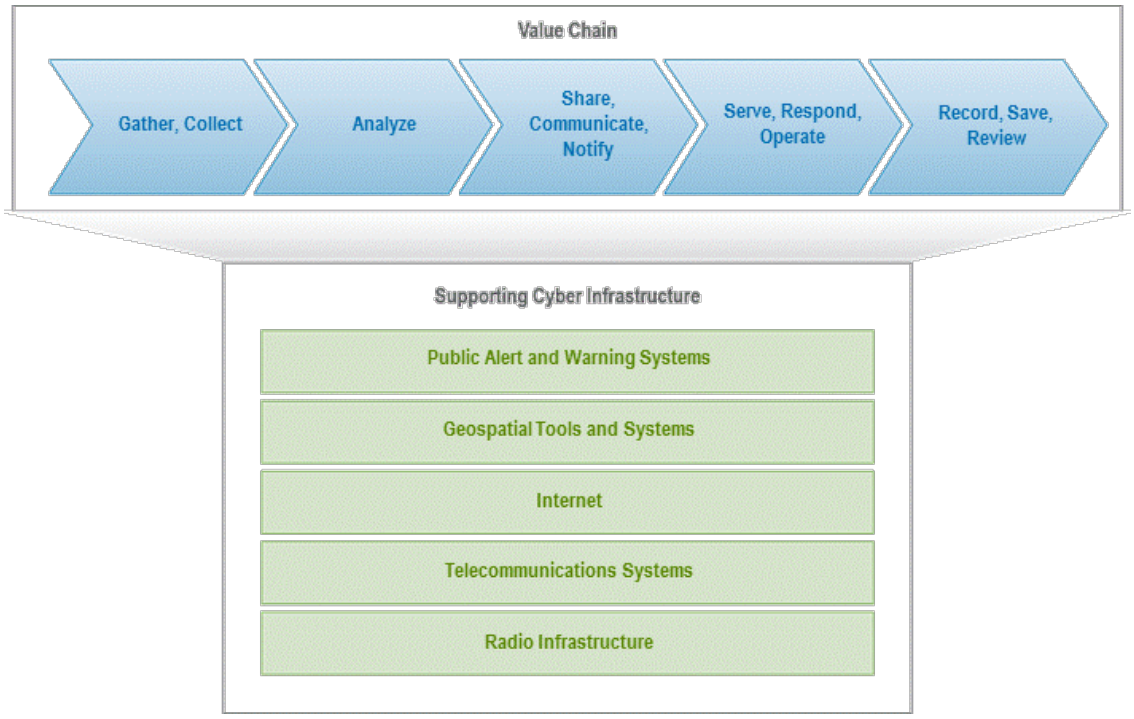

Figure 7: Public Works Supporting Cyber Infrastructure

3.6. Public Safety Communications and Coordination/Fusion

Table 7: Public Safety Communications and Coordination/Fusion Discipline

Discipline/Discipline	Description
Public Safety Communications and Coordination/Fusion	**Public Safety Communications:** This discipline serves several purposes. First, it is responsible for receiving and processing calls to 9-1-1 or other emergency telephone numbers when emergency services are needed. Second, this discipline coordinates and deploys law enforcement, firefighting, and EMS personnel to answer calls for help, and provides support to these field forces via land mobile radio (LMR) systems and computer aided dispatch (CAD) systems to assure the most appropriate response resources are sent to the correct location, based on response plans, service priorities, and resource availability. This discipline serves the citizen-to-authority communications access that the public requires when it experiences or witnesses an emergency; the authority-to-authority communications needed to achieve interoperability and maintain continuity of communications for first, second, and tertiary responders; and the authority-to-citizen communications needed when public alerting and warning systems are activated. **Public Safety Coordination/Fusion:** The coordination function also serves the purposes of collecting, analyzing, and disseminating data that may help emergency service responders or homeland security authorities prevent, detect, deter, disrupt, or respond to natural or technological threats that a locality, region, or State may face. It supports this purpose by operating fusion centers that gather raw or seemingly isolated data from open and secured sources and providing the analysis and distribution of information that can be used to intelligently connect people and events to help the members of the ESS to protect the public and the critical infrastructure upon which they rely.

Public Safety Communications

The PSC&C discipline represents the first link in the chain of emergency services delivery, which is the citizen-to-authority communications link. When members of the public require the aid of the sector, they require multiple access points based on where they are located, the means of communications they wish to use, and their personal ability to identify the correct agency and its points of contact to seek help.

To enable citizens to reach the appropriate public safety agency, a common national emergency telephone number was established. That number, 9-1-1, is routinely available in most parts of the country to citizens using landline or wireless telephones. Those calls reach the nearest available Public Safety Answering Point (PSAP), where a call taker receives and processes the call to determine where assistance is needed, the nature of the emergency, the details needed to assure that the most appropriate resources are dispatched from the proper agency, and then, in some areas of the country, provides pre-arrival instructions if needed to help callers take appropriate action to reduce their personal risk, preserve evidence, or render aid until first responders reach the scene.

The PSAP, or other emergency communications center receiving a call for help, also facilitates dispatch across multiple agencies, if needed, to meet the requirements of a safe and efficient emergency response. They may do this using computer aided dispatch systems, notification

systems, geographical information systems (GIS), interoperable communications systems, or any combination thereof. Across the United States, these activities take place tens of thousands of times every day.

Public Safety Coordination/Fusion

This discipline also supports coordination of information and resources. One common coordination method used is to operate fusion centers. A fusion center may incorporate professionals representing a wide variety of public safety and homeland security interests. These interests may include Federal, State, local, tribal, territorial, and non-governmental public safety agencies, law enforcement, homeland security, and emergency management agencies. The representatives of these interests and agencies collect data from a variety of open and secured sources to assess the risk that their area of responsibility may face as a result of emergency operations or disaster threats, criminal acts or terrorist threats, or other natural and technological factors.

These representatives collaborate to assess the information they collect to determine what, if any, links exist that may make any single factor a stronger threat if combined with multiple data points or risks. They seek meaning in what may seem to be disconnected acts, or they may identify trends that point to a need for escalation in notifications, planning, training, exercises, or response preparations. “Fusing” this data provides greater understanding, better situational awareness, and a common operating picture about threats and risks. It also allows distribution of an intelligible and credible message that can help prevent, detect, deter, disrupt, or respond to a threat. In this way, such centers provide value in protecting lives and critical infrastructurelocally, across a region, or throughout a State or States.

The array of cyber infrastructure that typically supports the PSC&C discipline is depicted in Figure 8. A description of the cyber infrastructure supporting the PSC&C discipline can be found in Appendix A.

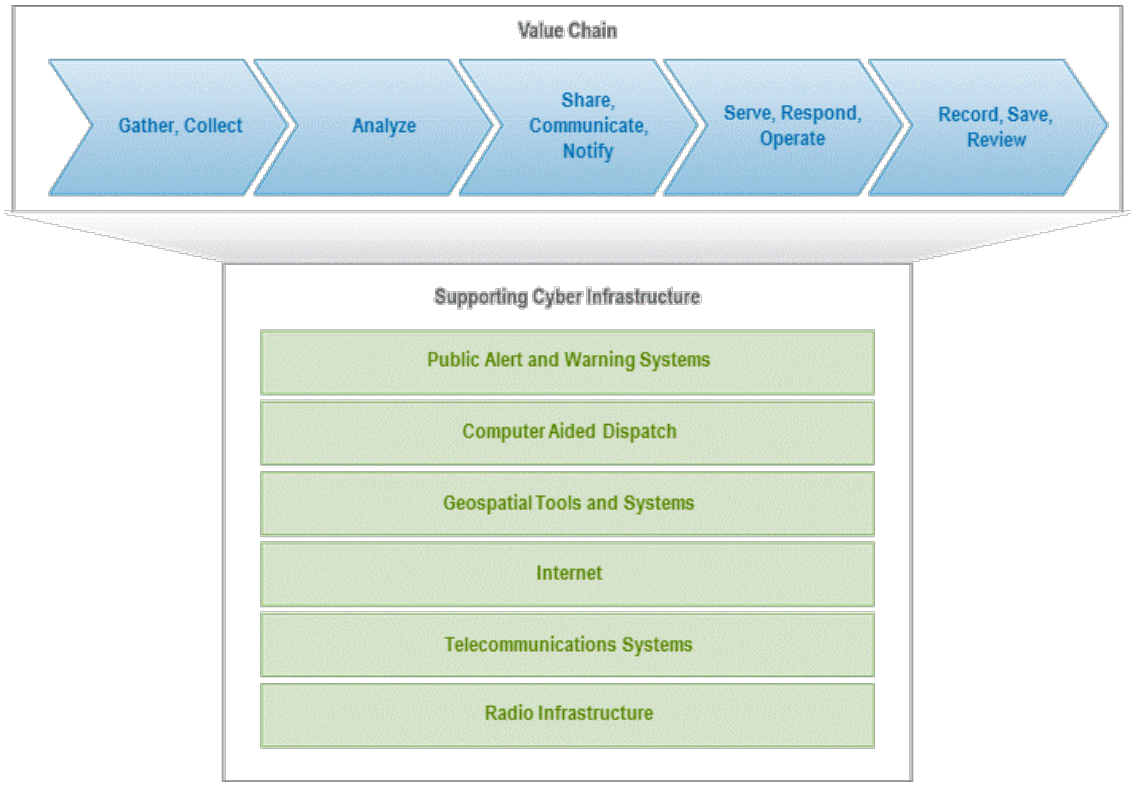

Figure 8: Public Safety Communications and Coordination/Fusion Supporting Cyber Infrastructure

4. EMERGENCY SERVICES SECTOR CYBER RISK PROFILE

4.1. Scenario Introduction

For the ESS-CRA, scenarios provided the primary means to identify and rate risks. Risk scenarios represent a distinct set of events that could significantly affect the ESS's ability to effectively perform its responsibilities. The scenarios allowed ESS-CRA participants to discuss practical real-life situations and determine threats, vulnerabilities, and consequences while allowing for consideration of compounding and overlapping effects often spreading across the multiple disciplines' cyber infrastructures.

4.2. Scenario 1: Natural Disaster Causes Loss of 9-1-1 Capabilities

Natural disasters are threats to ESS disciplines and their cyber infrastructure. Natural disasters typically affect specific geographic locations or regions and cause immediate impacts or degradation in normal day-to-day ESS cyber infrastructure and communications capabilities, including 9-1-1 capabilities. This scenario would have compounding consequences. Any natural disaster significant enough to render 9-1-1 communications inoperable is also likely to cause damage to property and potentially injury or loss of life to persons in the surrounding communities. The most catastrophic dimension of this scenario is the case where numerous customers are in need of 9-1-1 for assistance and the capability is unavailable via traditional communications means such as telephone. In this case, customers would be required to identify alternate methods of communication with ESS entities, or they would be required to physically go to the ESS entities' facilities.

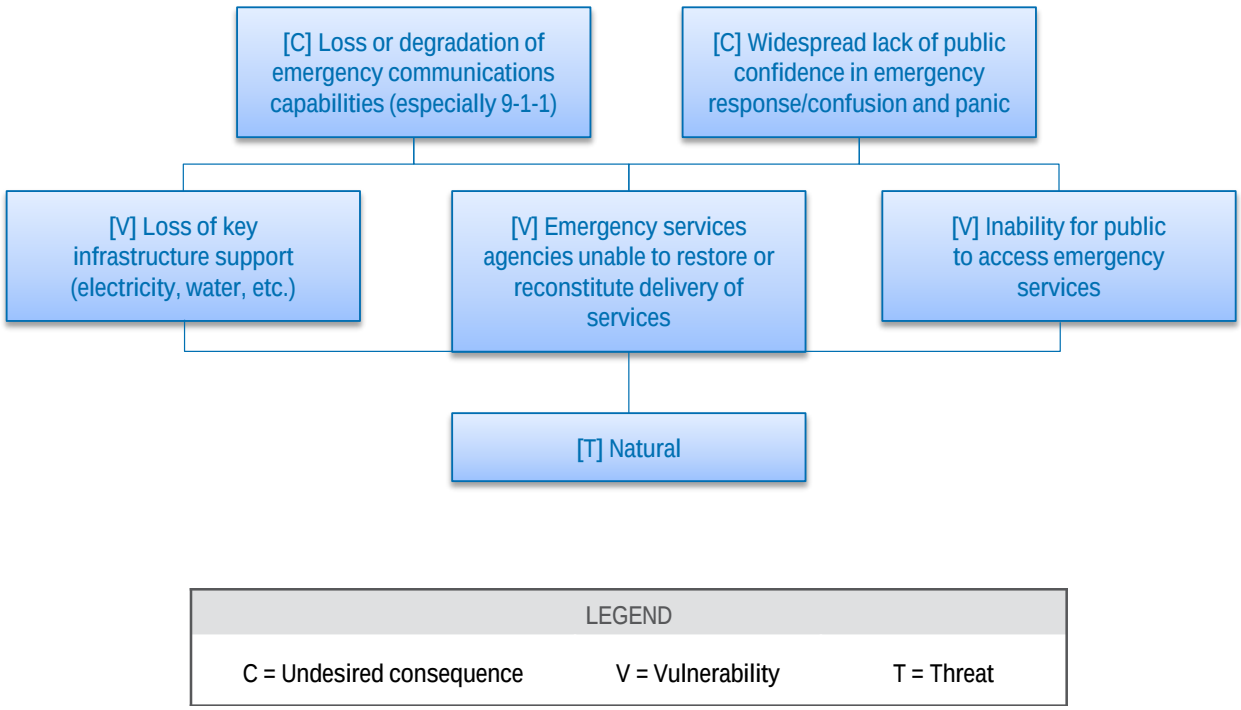

Figure 9: Scenario 1 Consequences, Vulnerabilities, and Threats

Specific disasters were not selected and rated because of the large geographic footprint of the United States; instead, the ESS-CRA evaluation assumes that a disaster that is most likely to affect a particular region or locale is significant enough to be deemed a federally declared natural disaster.[6]

The components of this scenario include undesired consequences, the vulnerabilities that can lead to those undesired consequences, and the threats that can exploit those vulnerabilities. The components are relevant to the following ESS disciplines: law enforcement, fire and emergency services, EMS, public works, and PSC&C. Figure 9 depicts the relationships among the consequences, vulnerabilities, and threats in the scenario. The following analysis evaluates the risks and identifies the impacts of a natural disaster causing the loss of 9-1-1 capabilities to the ESS disciplines and its cascading impacts.

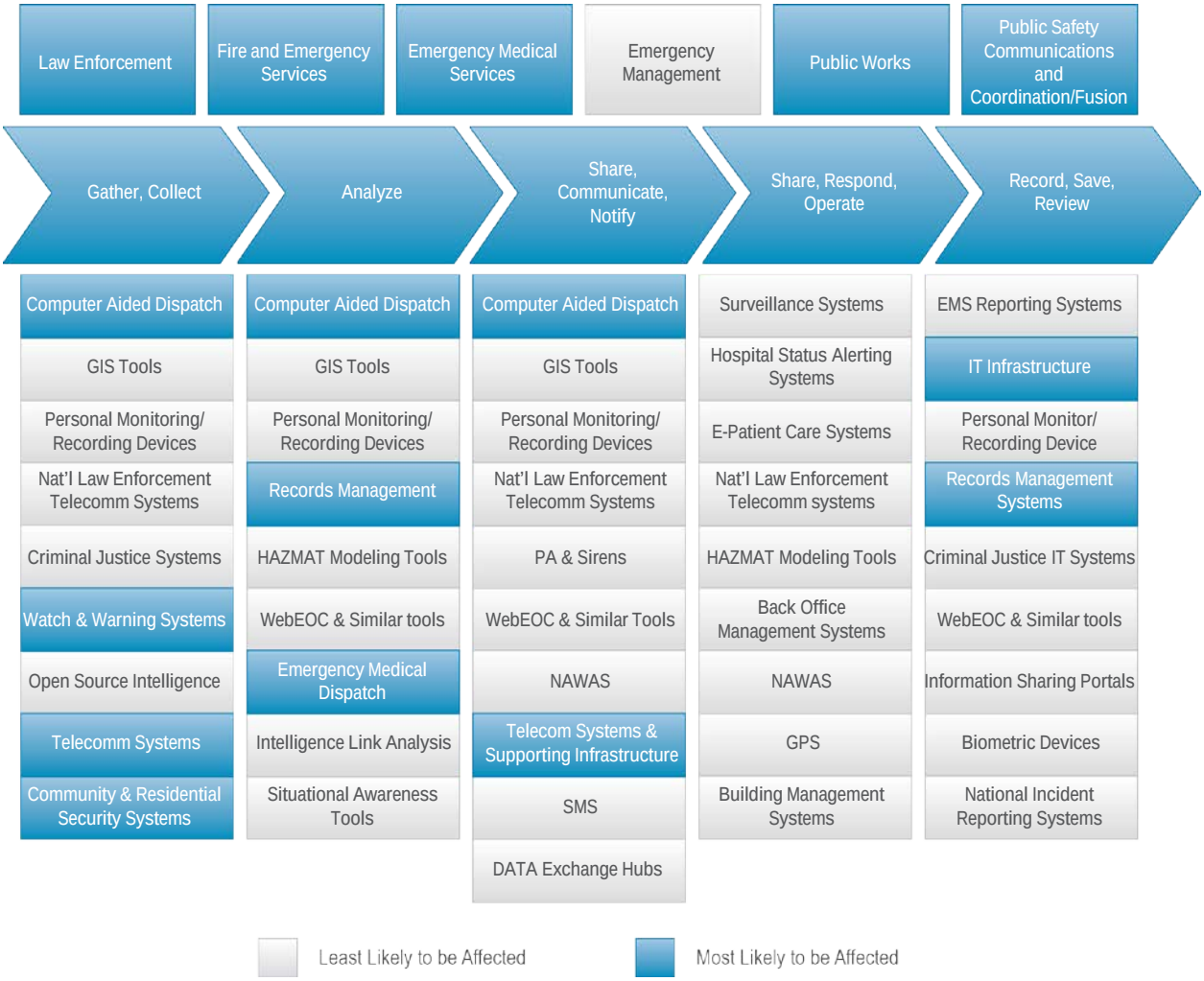

Figure 10: Scenario 1—Disciplines and Cyber Infrastructure Affected

[6] The Disaster Process and Disaster Aid Programs, http://www.fema.gov/hazard/dproc.shtm. Accessed on 12/12/2011.

Figure 10 shows how the ESS disciplines, value chain, and supporting cyber infrastructure are most likely to be affected by a natural disaster resulting in the loss of 9-1-1 capabilities. When a telecommunications system, such as 9-1-1 systems or CAD systems are degraded or inoperative, situational awareness by all parties across all disciplines is significantly affected, thereby reducing the likelihood of successful coordinated responses to emergencies.

Risk Assessment Scenario 1: Natural Disaster Causes Loss of 9-1-1 Capabilities

Figure 11 illustrates how this scenario affects ESS and its disciplines. The PSC&C, EMS, Fire and Emergency Services, and Law Enforcement disciplines are more negatively affected than the other two ESS disciplines—Public Works and Emergency Management. If a natural disaster, including meteorological, geological, or biological incidents, disables one or several PSAPs, or otherwise causes the loss of 9-1-1 capabilities, the operational capabilities across the ESS disciplines—including the Law Enforcement, Fire and Emergency Services, PSC&C, Public Works, and EMS—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 significantly affect the ability of ESS to perform emergency response.

It is a common practice across the ESS community to incorporate the concept of redundancy in 9-1-1 infrastructures. However, redundancy is not helpful in the face of significant natural threats if the redundant infrastructures are located in the same geographic area, as is the case for the majority of PSAPs. Backup PSAP functions may be limited to one PSAP located close to the primary PSAP. This scenario considers the possibility that natural disasters may be destructive enough to render both the primary and the redundant PSAPs insufficient to provide emergency communications services.

ESS entities provide essential services that seek to limit loss of life and damage. The degradation of ESS disciplines results in exposure of ESS entities' consumers to increased risks, leaving them to mitigate or respond to the situation themselves. This situation can trigger cascading consequences to public health and safety as well as greater economic and physical destruction. For this reason, the disciplines that perform emergency response capabilities are shown as having greater consequence impacts in Figure 11.

Figure 11: Relative Risk Profile of Scenario 1: Natural Disaster Causes Loss of 9-1-1 Capabilities

Natural Threat—Public Safety Communications and Coordination/Fusion

As previously noted, natural disasters are some of the most regularly occurring threats to the ESS in general, and to the PSC&C discipline specifically, because 9-1-1 capabilities are among the discipline's core services. 9-1-1 capabilities depend heavily on commercial communications infrastructure. Many citizens use Plain Old Telephone Service (POTS) and wireless networks to connect to 9-1-1, and many public safety call centers use these networks to connect to citizens, send critical dispatches, and coordinate efforts with first responders. Natural disasters frequently disrupt, damage, or destroy infrastructure in the commercial networks needed by the PSC&C discipline. In these scenarios, citizens may lose the ability to make calls (and therefore reach 9-1-1) and call centers may have outages caused by damage to their communications infrastructure or lines, or communications lines may become overwhelmed and lead to denial of service.

The natural threats that could cause this scenario are numerous and vary by region of the country, but some of the more prominent threats include earthquakes, hurricanes, and winter

storms. Other threats may include celestial events, such as geomagnetic or solar radiation storms that cause communications outages, or biological threats, such as epidemics or pandemics, which might not cause outages but could still degrade conditions as a result of resources being overwhelmed. Several key vulnerabilities could be exploited by these threats. Physical vulnerabilities include the concentration of assets and/or cyber infrastructure (e.g. telecommunications hotel or call center), location of key facilities and assets (e.g.communications lines, PSAPs, cell towers) in vulnerable geographic locations, and a lack of alternate routing for 9-1-1 call centers. There are also technological vulnerabilities such as poorly designed architectures with single points of failure or a reliance on commercial providers, and process-related vulnerabilities such as a lack of preparation, training, or exercises. The assessment rated each of these threats and vulnerabilities as high, resulting in a high likelihood. In fact, this scenario had the highest likelihood in the PSC&C discipline because these issues arise more frequently than in any of the other scenarios.

The direct consequence to the PSC&C is the loss of the ability to coordinate emergency response efforts or to deploy resources effectively. In addition, the consequences would cascade and be felt by other ESS disciplines and other sectors beyond ESS. Most notably, PSC&C sector service providers in the affected area would be required to deploy resources to restore lines and infrastructure that are critical to 9-1-1 services. The Healthcare and Public Health (HPH) Sector would also be affected, as it would be more difficult to provide emergency medical services.

The impact of this scenario is likely to be felt in a regional or local area as opposed to a national level. However, because of the severe impact and cascading effects that can occur in those affected local regions, the consequences were assessed to be high. Since this scenario has a high likelihood and high consequences, this risk was rated higher than any other risk.

Natural Threat—Fire and Emergency Services

Natural disasters create hardship and heartache for every person living or working in the affected area. Those persons experiencing the effects of a natural disaster first-hand may be facing the very worst moment of their lives as they find themselves or others in need of immediate assistance, whether it is the result of severe weather, earthquake, tidal wave, wildfire, or another naturally occurring phenomenon. Floods can submerge sensitive electronic equipment at telephone infrastructure sites. Wildfires can burn overhead telephone lines or spread from wooded areas into central office facilities. Earthquakes can sever buried telephone lines, topple telephone poles, or snap lines stressed by excessive movement. While these are some of the more prominent natural disasters to which telephone systems are vulnerable, they are not the only ones. If the infrastructure facilities have not been hardened against the effects of a natural disaster, or if the infrastructure itself lies in a geographical location that is susceptible to natural disasters (such as floods or earthquakes) with insufficient telephone route diversity and alternate switching, then the carriers responsible may be unable to quickly restore or reconstitute the level of service required to serve a given populace.

People who find themselves in need of help from one or more of the ESS disciplines require the ability to contact those disciplines. While some urban areas may retain fire boxes on their downtown street corners, and some buildings may provide manual pull stations designed to alert building occupants to evacuate while they also transmit an emergency signal to a fire alarm

communications center, most people require dial tone and telephone connectivity to summon their nearest fire and emergency services organization. For those people, their ability to notify authorities of their needs is tied to their local emergency number, or 9-1-1.

Connectivity and dial tone are resources provided by a competitive local exchange carrier to dial and connect with 9-1-1. To reach a 9-1-1 call taker, a caller must be able to use a landline or mobile telephone or enhanced special mobile radio device to dial the emergency number. If the caller has no dial tone, the call cannot be connected. If the infrastructure that supports the dial tone is damaged or destroyed, the call can neither be connected nor completed because components, such as telephone lines, central offices, or switches, are essential to carrying the call to its destination. As a result, callers may be left panicked and confused about what to do. They may not have the knowledge of the location of—or the ability to send for help to—the nearest fire and emergency services station to summon firefighters or emergency response personnel in person.

In addition to the communications infrastructure vulnerabilities that may have been revealed in the wake of a natural disaster, the fire and emergency services discipline has a critical dependency on the Communications Sector; in the event of a natural disaster, reconstitution of communications infrastructures is performed by the Communications Sector. However, there are similar risks that fire and emergency services organizations can experience. If the loss of 9-1-1 capabilities is caused by the damage or destruction of the 9-1-1 communications center, provisions may have been made to develop alternate locations to which 9-1-1 calls could be routed. However, for the majority of PSAPs, redundancy is extremely limited geographically, and the location of an alternate PSAP may be vulnerable to the same natural disaster that affected the telephone companies. Some organizations, particularly those that have migrated to digital, Internet Protocol (IP) based infrastructure, may already have alternate communications centers in place, but if they have not properly planned for the activation and maintenance of such facilities, they may find themselves ill-prepared to reestablish 9-1-1 services. Further, if the personnel expected to use alternate facilities have not been trained to migrate services to the alternate site and have never conducted exercises to develop proficiency in doing so, the chances of successfully transitioning from the damaged site to the alternate site are also significantly reduced.

Fire and emergency services organizations in parts of the country where natural disasters occur frequently may experience a higher likelihood of losing 9-1-1 capabilities. In California, for example, wildfires, earthquakes, high winds, and tsunamis present ongoing threats; however, there are no parts of the country in which a natural disaster has not, and will not again, occur. If a citizen is unable to reach the local fire and emergency services organization when needed, and the organization is unable to provide for connectivity with the communities they serve, the consequences place lives and property that have already been threatened by the natural disaster itself at an even greater level of risk. It is this high likelihood of a natural disaster's occurrence causing a loss of 9-1-1 capabilities that, when coupled with the severe consequences, make this the greatest threat to the fire and emergency services discipline.

4.3. Scenario 2: Lack of Availability of Sector Database Causes Disruption of Mission Capability

ESS cyber infrastructure includes databases and their supporting elements. 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 manmade unintentional threats.[7]

The components of this scenario include undesired consequences, the vulnerabilities that can lead to those undesired consequences, and the threats that can exploit those vulnerabilities. The components are relevant to all ESS disciplines but focus on the law enforcement and fire and emergency services disciplines. The consequences, vulnerabilities, and threats were identified in elicitation sessions with ESS stakeholders. Figure 12 depicts the relationships among the consequences, vulnerabilities, and threats in the scenario.

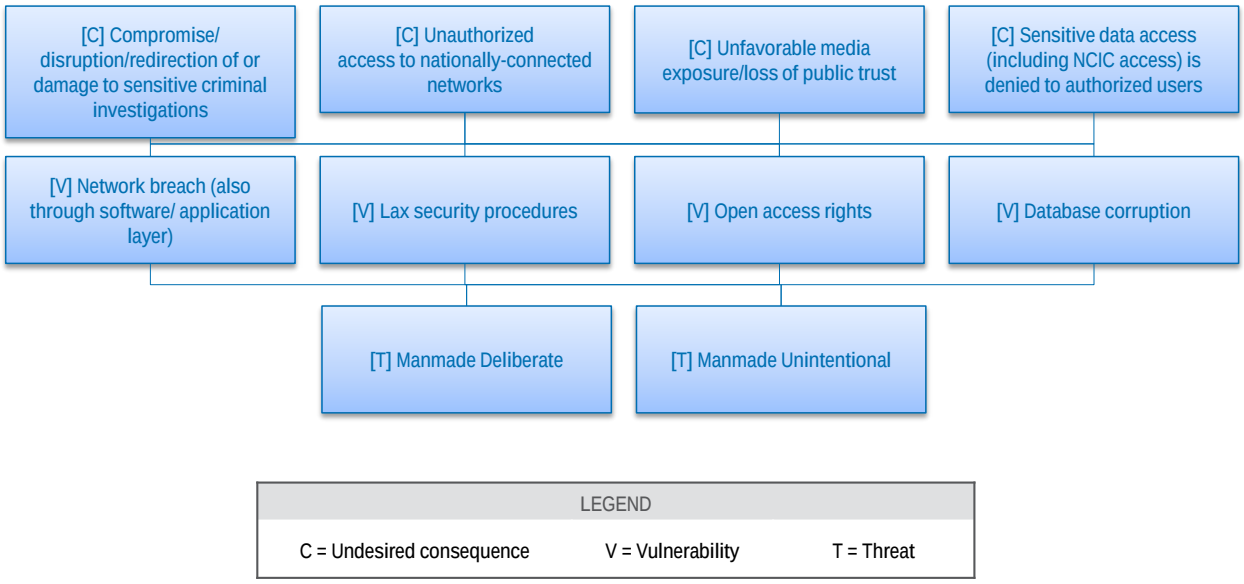

Figure 12: Scenario 2 Consequences, Vulnerabilities, and Threats

As demonstrated in Figure 13, a compromised sector database affects multiple disciplines, all elements of the value chain, and several systems and networks that support the value chain, particularly those elements providing information to first responders, including law enforcement personnel, firefighters, and emergency service personnel. Notably, in this scenario, law enforcement personnel could lose the ability to run accurate criminal background checks on suspects jeopardizing both their own safety as well as that of the general public. Law enforcement agencies would have to rely on more traditional methods of identification and criminal background checks such as using radio communications or mobile communications and

[7] Multiple types of attacks against databases are included in the 2010 Open Web Application Security Project Top 10 critical web application security flaws (https://www.owasp.org/index.php/Top_10_2010. Accessed on 12/14/2011.

relying on manual checks of State and local records. In addition, firefighters and emergency service personnel could lose access to data that would assist them in responding to an emergency, such as floor plan layouts, commercial building contents, documented hazards, and protocols and best practices to safely deal with various hazards. Firefighters and emergency service personnel would have to rely on printed materials on file, which are often out of date or inaccessible.

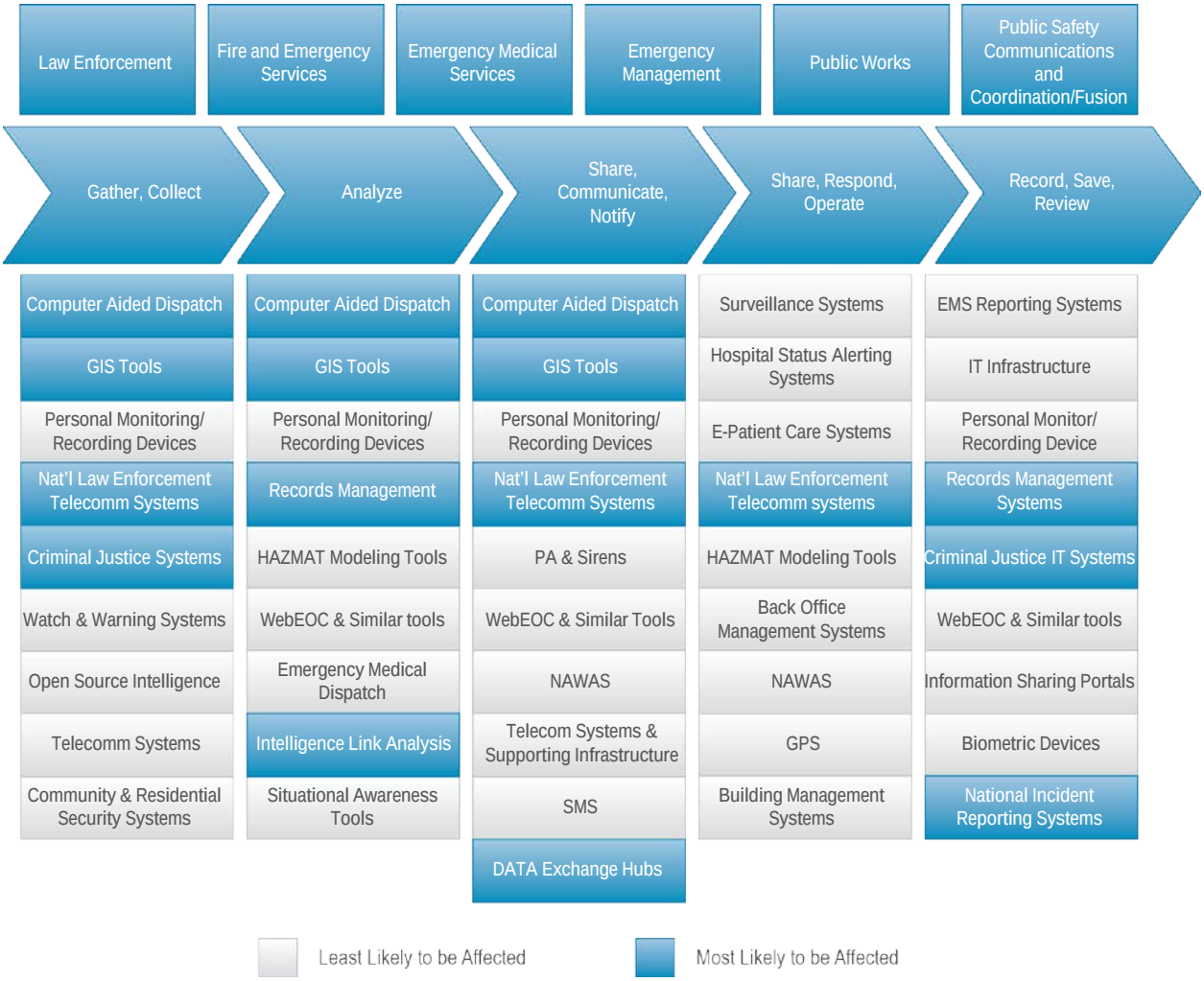

Figure 13: Scenario 2—Disciplines and Cyber Infrastructure Affected

Risk Assessment Scenario 2: Lack of Availability of Sector Database Causes Disruption of Mission Capability

A manmade deliberate attack against ESS databases is most likely to occur within the PSC&C, law enforcement, emergency management, and public works disciplines. As Figure 14 shows, of these four disciplines, PSC&C would be most affected by such an attack while the law enforcement, public works, and emergency management disciplines would experience relatively equal effects to their missions.

Figure 14: Relative Risk Profile of Scenario 2: Lack of Availability of Sector Database Causes Disruption of Mission Capability—Manmade Deliberate

As shown in Figure 15, the risk of manmade unintentional threats to ESS databases affects these four disciplines in a relatively similar manner. Namely, the PSC&C discipline would be most affected by such an incident, along with the public works discipline, which has a higher consequence rating than in the manmade deliberate scenario. The law enforcement discipline would experience relatively equal effects on its mission. In addition, in the manmade unintentional threats scenario, the EMS and fire and emergency services disciplines are at risk. The emergency management discipline's likelihood and consequence ratings are lower in the unintentional threat scenario.

Figure 15: Relative Risk Profile of Scenario 2: Lack of Availability of Sector Database Causes Disruption of Mission Capability—Manmade Unintentional

Manmade Deliberate Threat—Public Safety Communications and Coordination/Fusion (PSC&C)

The PSC&C discipline relies on various kinds of ESS databases, including criminal justice databases, such as the National Crime Information Center (NCIC) database; geospatial databases with critical infrastructure data; and motor vehicle administration databases. These databases are most notably in the sub disciplines of providing fusion center capabilities and providing GIS and CAD capabilities. While these databases are often owned and maintained by other ESS disciplines, such as public works, law enforcement, or fire and emergency services, the PSC&C discipline uses them to coordinate effective response operations among all of the ESS disciplines.

Potential threat actors who could deliberately cause this scenario include criminals, activist hackers (hacktivists), cyber vandals, and/or corrupt or disgruntled insiders. Malicious actors can be motivated by objectives that include obstruction, counterintelligence, and deception, such as

trying to embarrass an agency, looking for thrills, diverting attention from or adding to the magnitude of a separate attack, or eliminating certain records. Such actors may be part of a structured organization and have operational knowledge of technology that can be used to attack databases.

There are database vulnerabilities that malicious actors try to identify and take advantage of, especially if the database is linked to Web-based applications. According to SANS (SysAdmin, Audit, Network, Security) Institute, attacks against Web applications constitute more than 60 percent of all attack attempts observed on the Internet, and Structured Query Language (SQL) injections against databases account for nearly one-fifth of all security breaches.[8] In addition, several available open-source database vulnerability tools make it easy for the malicious actor to probe systems. The actor does have constraints, such as the need to be covert, a small window of time to execute the attack, and often a lack of insider physical or logical access to systems that include law enforcement databases. However, the capabilities and resources of this threat actor, combined with database vulnerabilities, make the malicious threat actor a key concern of the law enforcement discipline—mostly because of the consequences that can result from successful degradation of law enforcement personnel's access to the databases.

As a result, the risk likelihood associated with the scenarios ranges from low to medium, and the consequences range from low to medium-high. The manmade deliberate threat scenarios are higher impact than the manmade unintentional threat scenarios. The likelihood of an attack can also rise if a manmade deliberate threat actor targets a database with vulnerabilities caused by manmade unintentional threats such as untrained users.

While the relative consequence of this scenario can vary depending on the specific database targeted and the magnitude of the attack, the consequences for the PSC&C discipline could be very significant. Fusion centers and call centers are expected to maintain a high-level of performance at all times, and while these centers often have offline or paper backups, using those resources may slow or degrade their ability to deploy or coordinate efforts. For example, the loss of a GIS database may prevent a PSAP from identifying the location of a 9-1-1 caller, thereby slowing response time until a location can be identified manually. The loss of key databases may also prevent a dispatcher from receiving or responding to requests that are pending action in a CAD system. Consequences may also cascade to other critical infrastructure sectors, especially industries with a more critical dependence on response capabilities because of the nature of their activities (such as certain types of manufacturing or work with HAZMAT).

Given the serious consequences in this scenario, the impact could be significant, especially if it occurred in a highly populated area. The impact will vary based on the length and severity of the outage and could be mitigated through maintaining proper backups and effective training on how to respond during such an outage. In addition, it is important to note that while the risks from manmade deliberate and unintentional threats are similar, SMEs who provided input to this assessment judged that the likelihood of an unintentional threat causing the outage was slightly greater because of existing mitigations such as access control mechanisms and the greater access that authorized insiders have to such databases.

[8] SANS Top Cyber Security Risks, http://www.sans.org/top-cyber-security-risks/summary.php). Accessed on 1/30/2012.

Manmade Unintentional Threat—Emergency Medical Services

The greatest threat to ESS databases are unintentional acts, such as software design defects or programming failures. Other threats include the incorrect input of data or inaccurate modification or deletion of records. The latter circumstance can affect other mission-critical services, such as properly recording and saving patient care data or providing accurate medical billing. Another source for compromise can be unintentional disruption of critical databases. For example, the National EMS Information System (NEMSIS) is a national effort to promote the development of local, State, and national EMS patient electronic healthcare records and data systems.[9] At the national level, the goal of NEMSIS is to maintain a national EMS database. As of February 2012, the majority of States and territories have implemented a NEMSIS-based State EMS data system with 36 States and territories submitting NEMSIS data to the national EMS database.

As described below, people and process vulnerabilities are predominantly unintentional but can lead to compromised EMS databases.

- ***EMS providers, other employees, or third-party software and database specialists are the most likely persons to accidentally cause a database compromise.*** They may do so via acts of carelessness or recklessness, but other factors such as insufficient training or even power outages during programming or data entry can place these persons in the position of accidentally causing a database compromise. For example, database users can inadvertently corrupt their information when they reboot or shut down their access terminals while the database is open.
- ***Physical and environmental security factors, such as where and how access terminals are placed or used, can contribute to unintentional database compromises.*** Poor physical access control, exposure of equipment or software to trip hazards or drops, and lack of protection of power equipment are examples of physical and environmental security factors that can lead to disruption of information systems, including databases.

Depending on which database is compromised, the consequences will vary. It may take a short time to recognize a compromise in a database function, but it may take hours to reconstitute the data stored therein, unless effective redundancy is available. Even then, the cascading effects of some compromises, such as to medical billing, can delay vital revenue streams that sustain some EMS agencies. Other compromises may have more critical implications. For example, if the Master Street Address Guide in a CAD system is compromised, EMS response may be delayed or the request may be directed to the wrong agency or jurisdiction. If geospatial systems are compromised, such as Automatic Vehicle Location, it is possible that the closest EMS resources to an emergency may be overlooked and a more distant unit sent in its place. If online resources such as poison control experience a database compromise, the consultation may be inaccurate and treatment recommended either unreliable or even contraindicated.

Given these possibilities, while the risk of compromising a critical EMS database is low, the consequences for an EMS agency and perhaps even for its patients, are high.

[9] NEMSIS, http://www.nemsis.org/. Accessed on 2/10/2012.

4.4. Scenario 3: Compromised Sector Database Causes Corruption or Loss of Confidentiality of Critical Information

As stated in Section 4.3, ESS databases are critical to supporting sector missions and activities. In the case of a compromised sector database causing corruption or loss of confidentiality of critical information, there will be disruption to mission capabilities.

Corruption or loss of confidentiality of critical information residing on a database can be the result of a manmade deliberate threat (e.g., hacktivist, cyber-criminal) or a manmade unintentional threat (e.g., software or programming failure). Databases are frequently targeted in manmade intentional attacks. If those databases are not protected against unauthorized access and modification and are not regularly backed up, data loss or corruption can significantly impair ESS mission capabilities. The threats, vulnerabilities, and consequences in this scenario affect all six critical ESS disciplines. The ESS baseline risk assessment report assesses the impacts of the scenario on six ESS disciplines and provides the foundation for creating risk mitigation strategies.

Intentional or unintentional manipulation of law enforcement databases that causes or leads to data loss or corruption can jeopardize the operations of law enforcement resources such as CAD and criminal justice networks and systems. Detecting such an incident that affects availability will likely take a matter of minutes in the case of data corruption but it may take hours to return service to a minimally acceptable level. An incident that corrupts the information of a database may take longer to recover from, depending on the frequency and availability of information backups. Loss of data confidentiality may take longer to detect depending on the sophistication and goals of the threat actor. If the threat is unintentional, the impact may be mitigated quickly by undoing actions that caused the incident or restoring data.

An incident occurring as a result of a deliberate threat actor may take longer to mitigate. Depending on the databases and associated systems attacked, the impacts of an attack may cascade to consequence areas such as homeland security. For example, the court system may be affected by an attack on related databases, foreign operations with Interpol may be delayed, and Medicaid billing/financial management can be impaired. Public health and safety may be affected if law enforcement and fire databases impair fire and search and rescue missions.

As noted in the analysis for Scenario 2, a malicious actor can use numerous database vulnerabilities, especially if the database is linked to Web-based applications. The man-in-the-middle attack is a common hacker attack and can be used to acquire database credentials. There are also several available open-source database vulnerability tools that make it easy for the malicious actor to probe systems.

The components of Scenario 3 include undesired consequences, the vulnerabilities that can lead to those undesired consequences, and the threats that can exploit those vulnerabilities. The components are relevant to the following ESS disciplines: law enforcement, fire and emergency services, EMS, emergency management, public works, and PSC&C. The consequences, vulnerabilities, and threats were identified in elicitation sessions with ESS stakeholders. Figure 16 depicts the relationships among the consequences, vulnerabilities, and threats in the scenario.

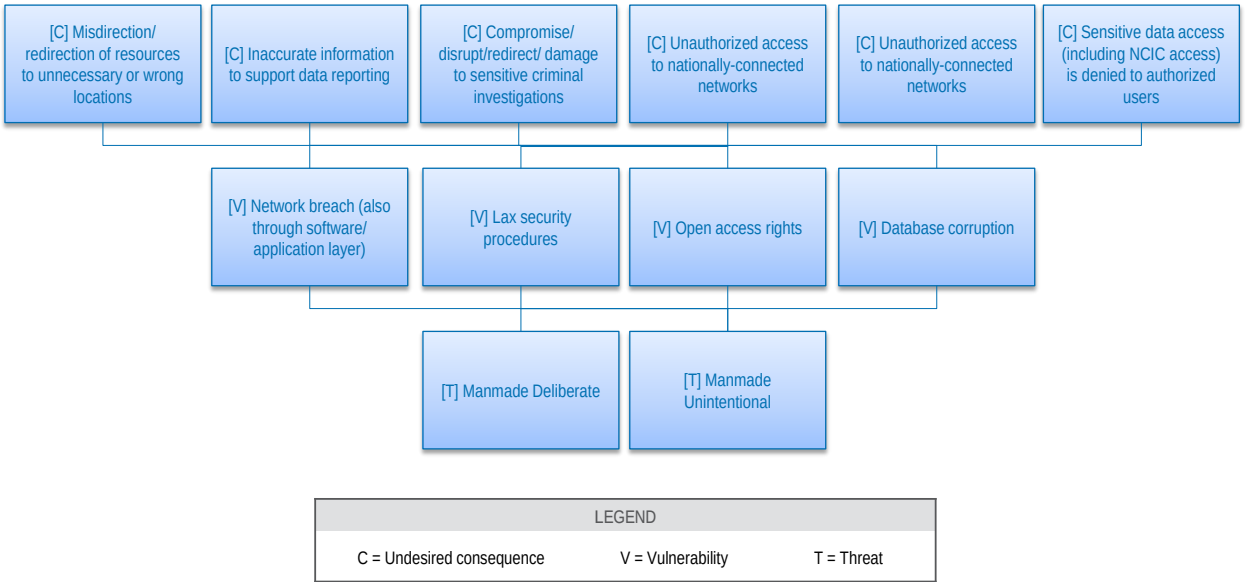

Figure 16: Scenario 3 Consequences, Vulnerabilities, and Threats

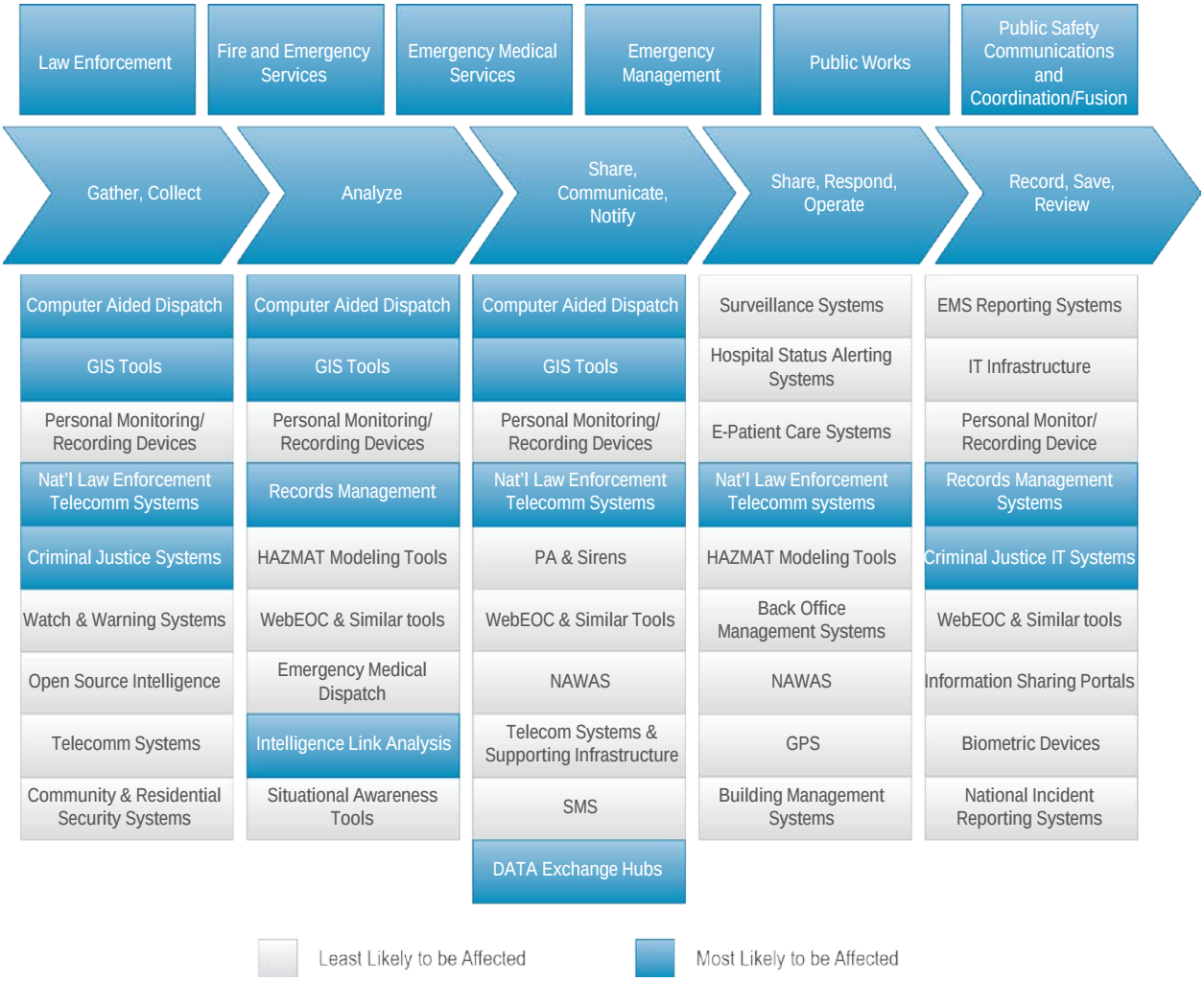

Figure 17: Scenario 3—Disciplines and Cyber Infrastructure Affected

As Figure 17 illustrates, a compromised sector database that causes the corruption or loss confidentiality of critical information can have a significant impact across ESS. Incorrect or corrupt data can place public safety agencies, first responders, and the general public in significant jeopardy.

Law enforcement agencies, in particular, rely extensively on the accuracy of criminal and other public safety databases used to verify a person's identity and/or criminal record. If this information were to become corrupted or stolen, law enforcement processes could be significantly delayed and criminal organizations may be enabled to perform counter-intelligence operations. Moreover, if frontline first responders feel that the information that they are getting from various public safety databases is in some way inaccurate, they will lose confidence in the system, thereby rendering it less effective.

The other ESS disciplines are affected by the scenario because—similar to law enforcement—they rely on shared data sources and information to improve their situational awareness, coordinate response and operations, and manage communications and coordination tools. For

example, each discipline uses GIS systems as a tool in conducting their activities. If GIS data is inaccurate or corrupted—deliberately or unintentionally—response agencies could be dispatched to the wrong destination; thereby, putting the entity or individual needing the emergency response at risk of further harm.

The public works discipline uses databases to support capabilities such as geospatial tools and systems that store critical infrastructure information. These types of databases store information related to utility placement, facility types and locations, vehicle locations, and navigational aids. Other databases may store information related to resource inventories, employee records, or agency payrolls. The information contained in these databases can be analyzed to identify resource needs or infrastructure disruption trends to ensure the function is properly maintained. The increased connectivity provided by IP-based systems and wireless devices has now made it possible for this information to be shared with connected devices, such as computers, smartphones, or Global Positioning System units, to provide public works employees with instant access to the data needed to sustain the function's operations. In addition, these devices are able to record and transmit information to the databases, ensuring the information contained within is updated and accurate.

Although the emergency management discipline can support some public works discipline operations during an emergency, such as field operations, the corruption of critical information resulting from a database compromise could cause redirection of public works resources and slow incident response times. Dispatches could be misdirected or utility services, such as electricity, water, or wastewater, could be lost depending on the type of database involved. The increased adoption of information technology (IT), and the corresponding IT security culture, has increased the discipline's awareness of IT-related incidents so that detection of such an event could be measured in hours. The rapid detection of a compromised database allows for recovery within a few hours and reconstitution of the discipline's operations can be achieved within a few days. The cascading impacts on other sectors would be slight and limited to those sectors that play a role in utility services, such as the Energy and Water Sectors. The database vendor and the agency involved in the incident would face substantial public confidence impacts in the local area affected but not at the national level.

Risk Assessment Scenario 3: Disciplines and Cyber Infrastructure Affected

Figure 18 shows that in the case of a manmade deliberate scenario, the likelihood of the threat exploiting the vulnerability is generally low but the consequence varies from low to high across the ESS disciplines. The PSC&C and law enforcement disciplines have a higher consequence because deliberate corruption or stealing of data may have a more significant impact on day-to-day operations. For example, corrupted data in a law enforcement database or information leaked to the public can delay and impair criminal investigations. In the case of a manmade unintentional threat, the likelihood of the scenario is lower for the law enforcement and emergency management disciplines because of the emphasis on integrity of the data.

Conversely, the likelihood of the manmade unintentional threat, as shown in Figure 19, is higher for the fire and emergency services, EMS, public works, and PSC&C disciplines because of their transactional time-sensitive data operations. Overall, the consequences for manmade unintentional threats are slightly lower because databases have built-in processes to prevent

unintentional deletion or modification of large amounts of data and data is generally periodically updated.

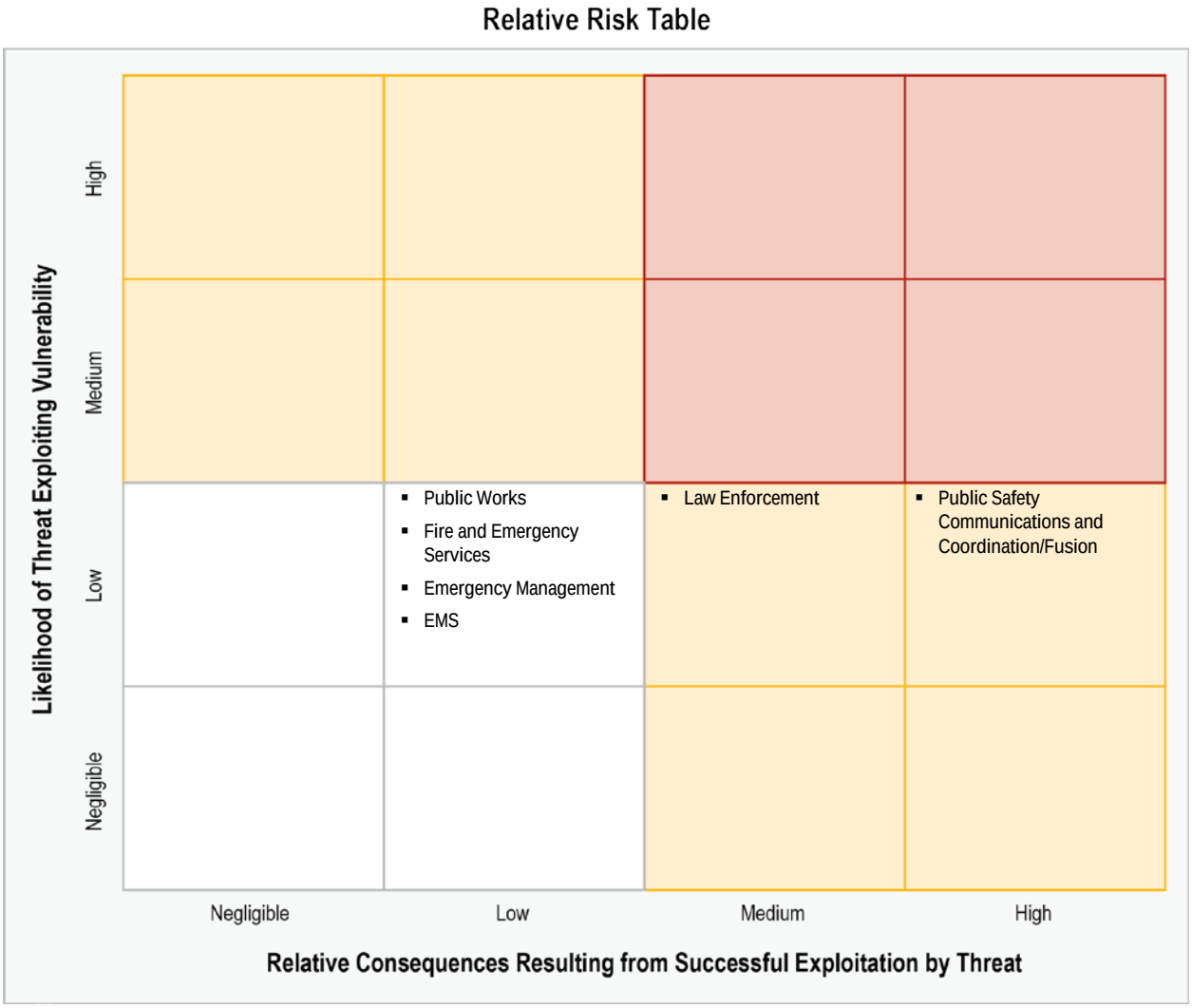

Figure 18: Relative Risk Profile of Scenario 3: Compromised Sector Database Causes Corruption or Loss of Confidentiality of Critical Information—Manmade Deliberate

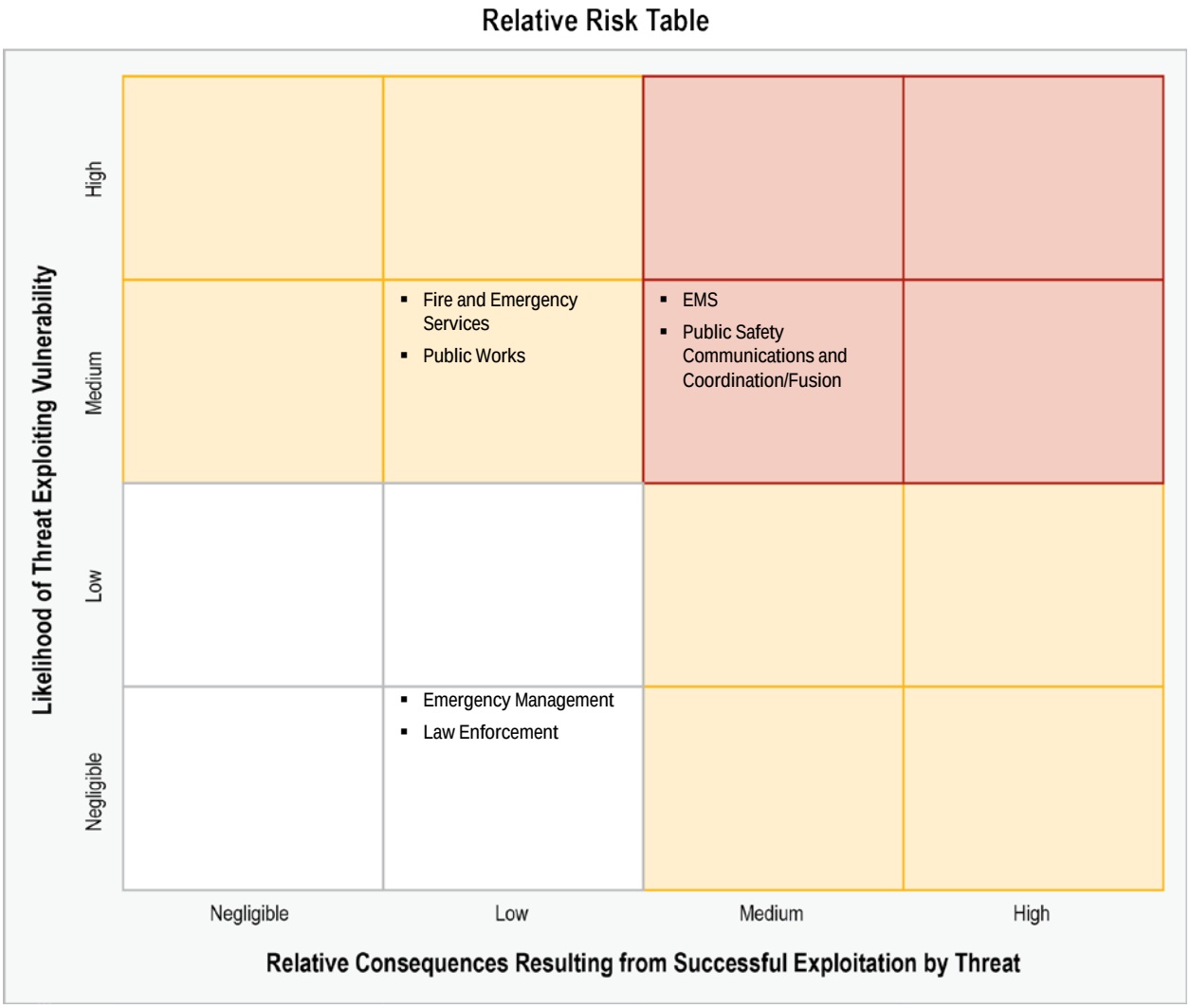

Figure 19: Relative Risk Profile of Scenario 3: Compromised Sector Database Causes Corruption or Loss of Confidentiality of Critical Information—Manmade Unintentional

Manmade Deliberate Threat—Law Enforcement

The ESS Law Enforcement discipline uses databases to assist in several activities, including managing personnel and equipment, conducting criminal investigations, gathering and protecting evidence, and apprehending perpetrators of crimes. Databases support cyber technology resources like CAD and criminal justice networks and systems. For example, in criminal justice networks and systems, databases support analysis to find commonalities that may have investigative value, such as patterns in sites of crimes, or names that recur from contacts at crime scenes. Fingerprint and identification databases provide rapid analysis of electronic print cards to search for suspects with prior criminal justice contacts. Databases are used by law enforcement agencies to enter, modify, and withdraw data. NCIC, for example, requires that the State police agency in every State audit the local, State, and tribal law enforcement agencies to assure that only staff that is trained, certified, and authorized are accessing the system, that

record keeping is organized and up-to-date, and that all entries meet Federal Bureau of Investigation (FBI) criteria.

Intentional or unintentional disruption of law enforcement databases can jeopardize the operations of law enforcement resources such as CAD and criminal justice networks and systems. The time to detect such an incident that affects availability will likely take a matter of minutes but it may take hours to return service to a minimal acceptable level. If the threat source is unintentional, the impact may be mitigated quickly by undoing actions that caused the incident or restoring data. An incident occurring as a result of a deliberate threat actor may take longer to mitigate because of the threat actor's/actors' desire to conduct the attack undetected.

Attacks on law enforcement database may be used as a basis for attacks on more secure networks such as Law Enforcement Online. Depending on the databases and associated systems attacked, the impacts of an attack may cascade to other critical infrastructure sectors. For example, the court system may be affected by an attack on related databases, foreign operations with Interpol may be delayed, and Medicaid billing/financial management can be impaired. Public health and safety may be affected if law enforcement databases impair fire, search and rescue missions. If the attack is reported publically, it may reduce the confidence in the government to perform its essential tasks. In addition, if the attack is reported publically, it may reduce the confidence in the government to regulate law enforcement.

This analysis focuses on deliberate threat actors because the consequences of a deliberate threat actor will likely result in a higher consequence to the sector. Major potential manmade deliberate threats to databases shared by multiple jurisdictions are cyber criminals and organized crime. These malicious actors would be motivated by objectives that include obstruction, counterintelligence, and deception. Such actors would likely be part of a structured organization and have operational knowledge of technology that could be used to attack databases. The actors do have constraints, such as the need to be covert, a small window of time to execute the attack, and often lack of insider physical or logical access to systems, including law enforcement databases. However, the capabilities and resources of these threat actors, combined with database vulnerabilities, make this a significant concern of the law enforcement discipline.

Like cyber criminals, organized crime actors can be motivated by objectives that include obstruction, counterintelligence, and deception. Such actors may be part of a structured organization and have operational knowledge of technology that can be used to attack databases. Cyber vandals or radical activists are the additional threat actors associated with manmade deliberate incidents expressed in this scenario. Thieves may also be interested in the proprietary information contained within some databases such as those within public works agencies. For cyber vandals and radical activists or hacktivists, corrupting a public works database could be a means to exert influence over government operation and draw attention to their cause (e.g. hacking groups "LulzSec" and "Anonymous").

Such threat actors typically understand the underlying technology, tools, and methods needed to compromise and corrupt the database, and can quickly create new attacks to adapt to the database involved. As discussed in Scenario 2, there are several database vulnerabilities that malicious actors can identify and leverage. These vulnerabilities not only lead to loss of availability, but can also result in compromise of database integrity and confidentiality. For example, the hacker

group LulzSec claimed it used a SQL injection attack against Sony Pictures in 2011 to steal user data of more than 35,000 users.

The risk likelihood associated with the scenarios ranges from low to medium, and the consequences range from low to medium-high. The manmade deliberate threat scenarios are higher impact than the manmade unintentional threat scenarios. The relative consequences can vary depending on the specific database targeted and the magnitude of the attack. The likelihood of an attack can also increase if a manmade deliberate threat actor targets a database with vulnerabilities caused by manmade unintentional threats such as untrained users.

Manmade Unintentional Threat—Emergency Medical Services

Unlike the other disciplines in the ESS, EMS agencies operate under a variety of models that include for-profit corporations, non-profit corporations, and not-for-profit organizations. The need to capture critical data to support these models is just as varied and depends on whether the agency charges patients (directly or indirectly) for their services. The databases that agencies using these models build, maintain, and operate may support—

- Business interests such as accounts receivable and accounts payable and fleet maintenance records
- Patient care such as electronic patient care reporting systems and approved medical treatment protocols
- Defined service areas, such as a Master Street Address Guide
- Receiving facilities such as status of capabilities and points of contact for free-standing emergency facilities, general hospitals, and specialized sites such as burn centers
- Training and licensing such as qualifications for personnel, certifications and expiration dates, and licenses to practice.

An example of an EMS database is NEMSIS.[10] As mentioned in Scenario 2, the goal of NEMSIS is to develop and maintain a national EMS database that includes local, State, and national EMS patient electronic healthcare records and data systems.

Although the risks that an EMS database may face are similar to the risks that other functional databases may encounter, the emphasis of many of the databases on which EMS agencies rely is limiting liability to the agency and promoting an effective and accurate accounting of patient care when transferring responsibility for a patient to another EMS agency. One scenario in which this could be important is when an ambulance crew delivers a critically injured patient to a landing zone, so that a waiting helicopter can provide rapid medical evacuation to a trauma center. This would also be important at a receiving facility when the patient care is turned over to a physician or nurse at a hospital's emergency department. While those interests may be behind the creation of many EMS databases, the business interests that a database supports may include the record-keeping necessary to remain solvent through accurate billing and accounting for payments received. Thus, when any of these databases is corrupted, the loss of access to essential data can affect the ability of an agency to pay for fuel, supplies, and insurance so that its

[10] NEMSIS, http://www.nemsis.org/. Accessed 2/10/2012.

ambulances can respond to calls, the ability to identify the best hospital to which a patient in need of specialized care should be transported, and the ability to optimize the pre-hospital care that trained and equipped emergency medical care providers can deliver en route to a hospital. Finally, if the patient care reporting system is corrupted, it can delay or cause deferment of better care for very ill or seriously injured patients because hospital staff cannot reliably account for the medical interventions taken by emergency medical care providers before their arrival with the patient.

There are several likely sources for an unintentional compromise of a database that cause the corruption of critical information. These sources of these vulnerabilities may include—

- **Personnel.** EMS providers, agency administrators, and third-party contractors (e.g. billing agencies, database and software engineers and administrators, and hardware technicians) may inadvertently cause database corruption when they use incorrect keystrokes, make inaccurate entries or modifications of data, or use a corrupted formula that misaligns or otherwise renders data unreliable.
- **Processes.** Improperly trained personnel, personnel who are fatigued from emotionally and physically demanding incidents, personnel who may be working under highly stressful conditions, and personnel who are operating under poorly maintained or enforced security policies have been exposed to a process vulnerability that could cause an unintentional database corruption.

The threat of a database being unintentionally corrupted stems from behaviors such as poor training or trained personnel applying their skills improperly, carelessly, or even recklessly. A technical flaw may also unintentionally corrupt a database. Other sources for corruption include power failures or surges, and even lightning strikes.

Fortunately, the likelihood of an unintentional corruption to a database containing critical information is low; however, the consequences of such instances are very high. Agencies could lose revenues essential to operating a viable EMS delivery system, but more significantly, the affected EMS agency could be exposed to civil liability and the public or the hospitals they serve could be exposed to errors in patient care.

4.5. Scenario 4: Public Alerting and Warning System Disseminates Inaccurate Information

Public alerting and warning systems contribute to several ESS disciplines' operational capabilities. These systems range from the national-level Integrated Public Alert Warning System for major emergencies to regional and local alert and warning systems. These systems provide alerts for a variety of events and ESS disciplines. Both older and newly modernized public alerting and warning systems can be at risk for either intentional or unintentional dissemination of inaccurate information. The ESS disciplines targeted in this scenario are emergency management, PSC&C, public works, and law enforcement.

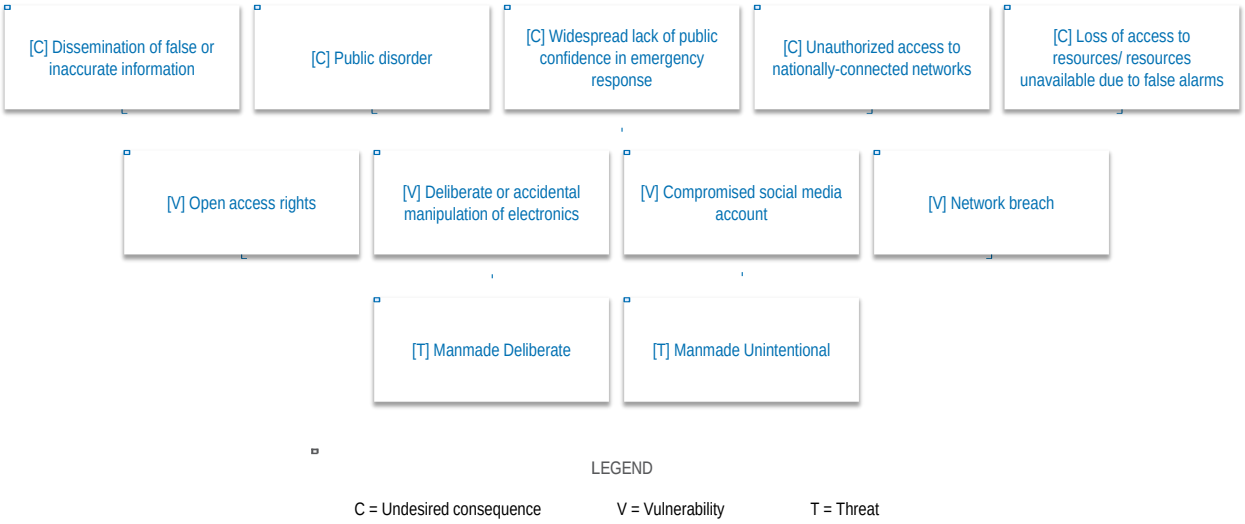

Figure 20: Scenario 4 Consequences, Vulnerabilities, and Threats

The components of this scenario include undesired consequences, the vulnerabilities that can lead to those undesired consequences, and the threats that can exploit those vulnerabilities. The consequences, vulnerabilities, and threats were identified in elicitation sessions with ESS stakeholders. Figure 20 depicts the relationships among the consequences, vulnerabilities, and threats in the scenario.

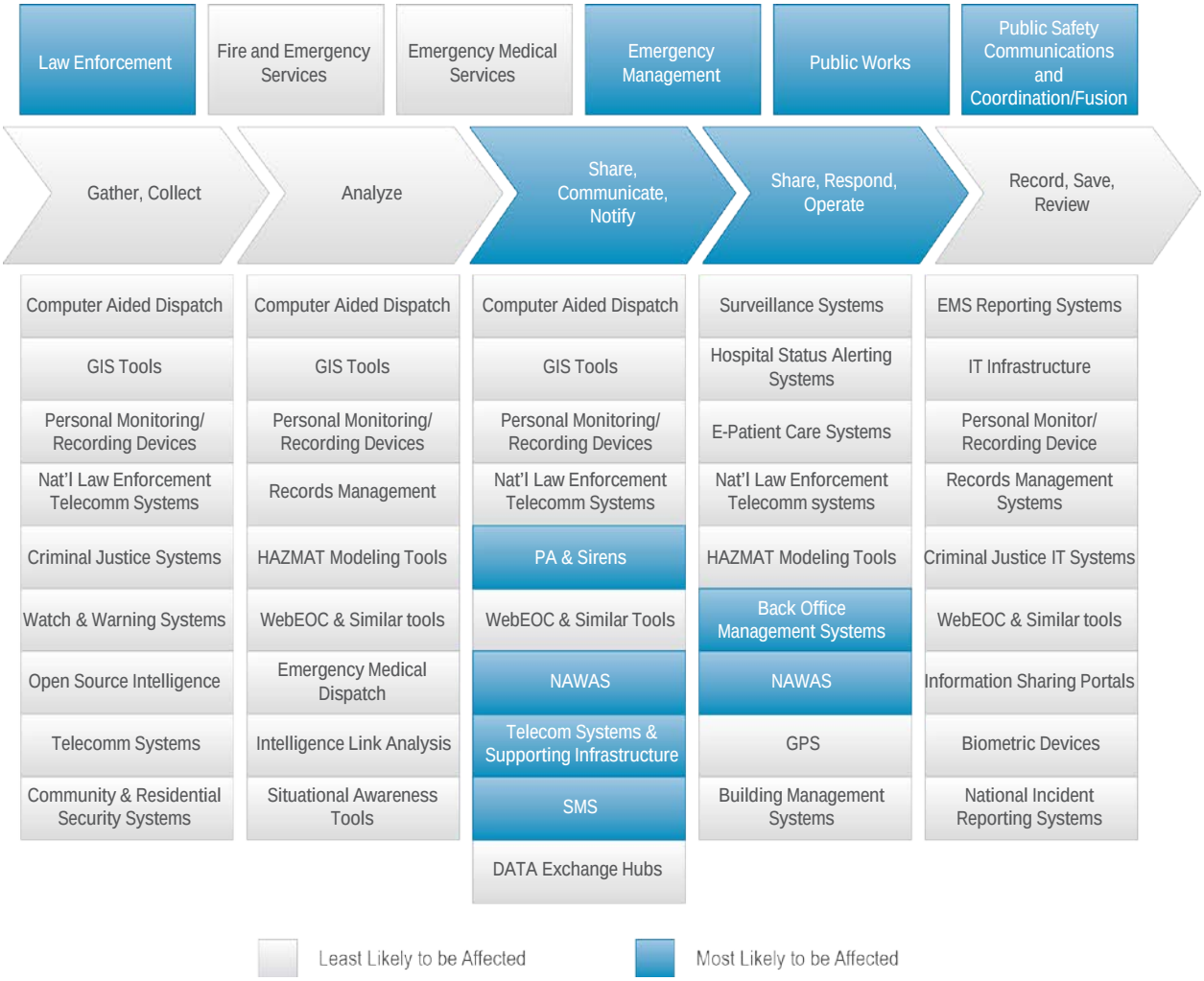

Figure 21: Scenario 4—Disciplines and Cyber Infrastructure Affected

As Figure 21 illustrates, when a public alerting and warning system disseminates inaccurate information, the Share, Communicate, Notify portion of the value chain is the most severely affected. When a public alerting and warning system disseminates inaccurate information, it not only creates unnecessary panic, but can also cause the public to lose confidence in the various public alerting systems and lead to the public ignoring an actual emergency because it is believed to be false. If this occurs, emergency managers will need to use other less efficient, improvised methods such as door-to-door notification, live TV, and/or radio announcements.

Risk Assessment Scenario 4: Public Alerting and Warning System Disseminates Inaccurate Information

Figure 22 shows that in the case of a manmade deliberate threat in this scenario, the likelihood of the threats affecting the ESS disciplines is low to medium, with an emphasis on the law enforcement discipline and emergency management, which will likely have to directly deal with the event in this scenario and its subsequent reactions. The relative consequence for several of

the disciplines, including law enforcement, emergency management, and PSC&C, is high because the public is likely to believe and react to information from a public alerting and warning system.

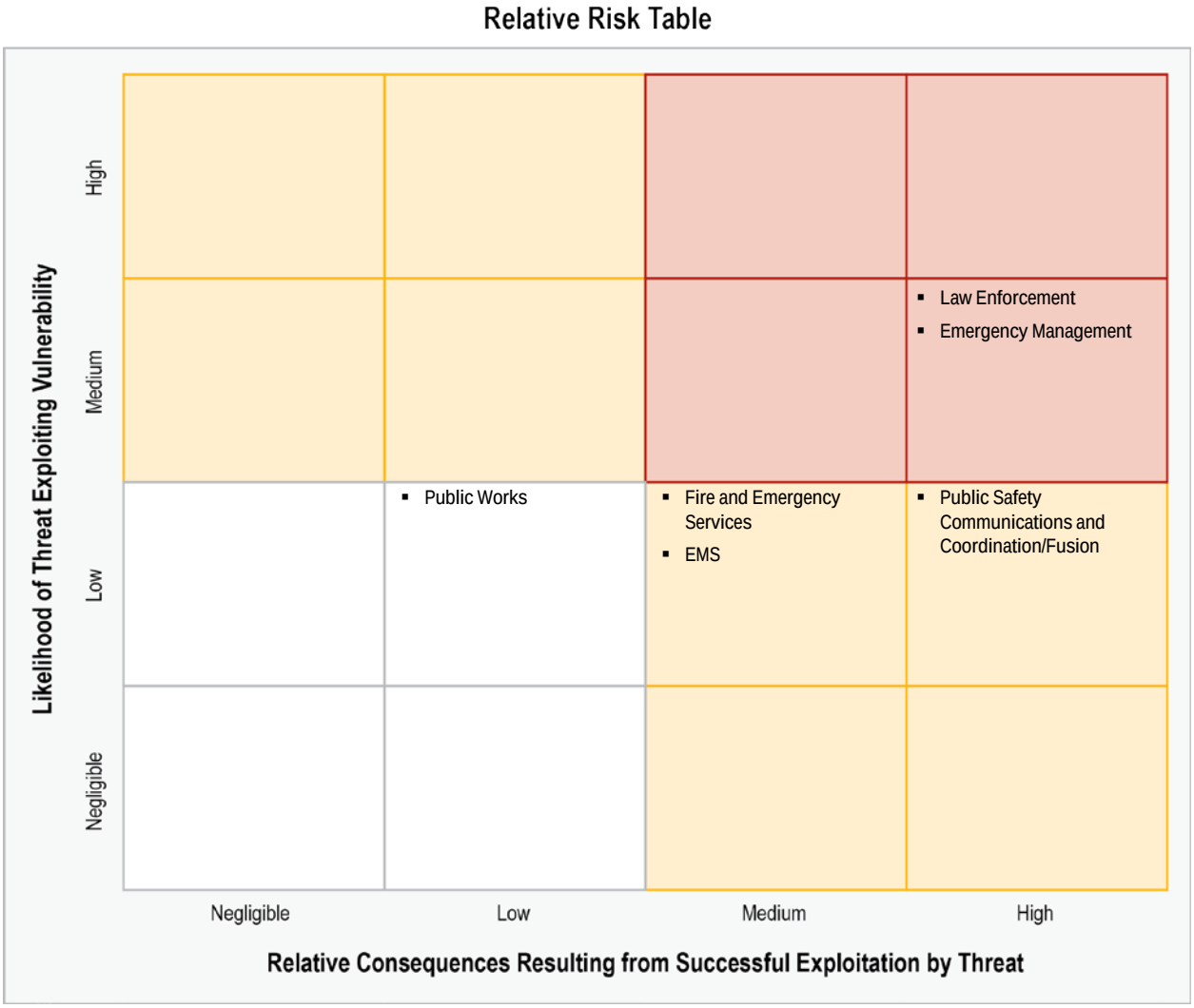

Figure 22: Relative Risk Profile of Scenario 4: Public Alerting and Warning System Disseminates Inaccurate Information—Manmade Deliberate

In the case of a manmade unintentional threat as shown in Figure 23, the likelihood of the risks in the scenario is generally higher for the ESS disciplines and the consequences are roughly the same or slightly lower. A manmade unintentional threat may be more common because of the potential for human error and technical error. However, unintentional threats may be detected and mitigated more quickly if the user associated with the unintentional threat is immediately aware of the incident.

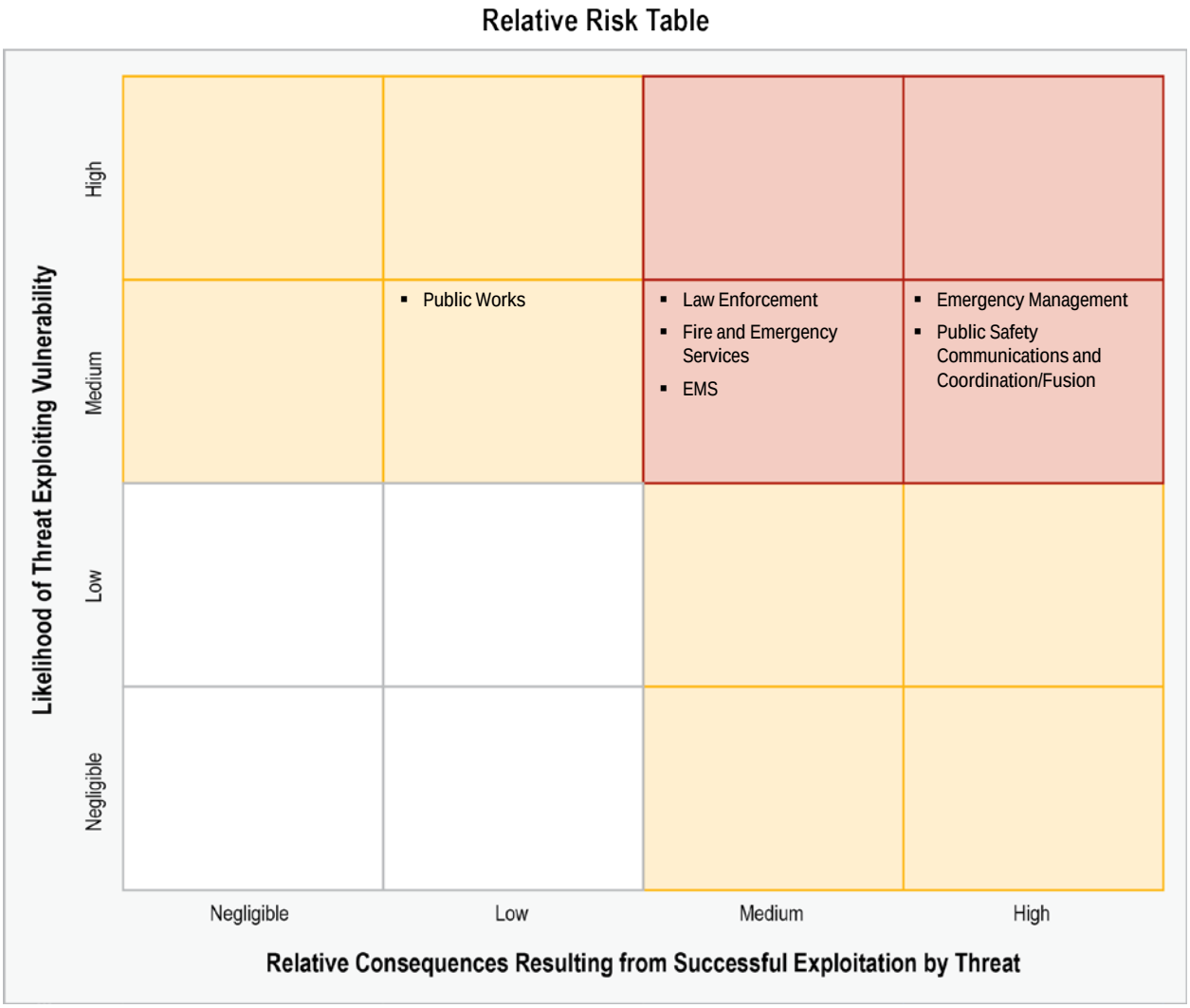

Figure 23: Relative Risk Profile of Scenario 4: Public Alerting and Warning System Disseminates Inaccurate Information—Manmade Unintentional

Manmade Deliberate Threat—Emergency Management

Emergency management professionals rely on a small number of systems to perform their disciplines, and public alert and warning systems are one of the more important types. The emergency management community is the "power user" group of public alerting and warning systems. They use systems such as the Emergency Alert System (EAS), emergency alert networks that disperse information to citizen subscribers via their registered devices (e.g., cellular telephones and pagers), sirens, and public address systems. Some agencies use Reverse 9-1-1® or similar products to send warnings to entire communities when the need arises. Public alerting and warning systems primarily support the following core activities of the emergency management value chain: share, communicate, notify; share, respond, operate; and record, save, review.

These alerting and warning systems use software that may be dependent on other cyber communications resources to disseminate their messages, such as telephony, telecommunications services, and the Internet.[11] EAS is commonly used to alert the population to severe weather warnings, when evacuations may be ordered in response to flooding or HAZMAT emergencies, or to simply conduct tests to assure that the system is operational and capable of disseminating information when needed. More automated or sophisticated public alerting and warning systems are used in real time to issue warnings, such as using sirens that are activated when a tornado is approaching a community. Public address systems may be used in downtown business districts or on college campuses, where significant pedestrian traffic in public areas make using loudspeakers to issue official news and directions a practical method. Some systems generate permanent records when they are used, while others do not.

Due to the wide reach of EAS and other alerting and warning systems and because their intended use is as an early warning and mitigation system, the consequences of inaccurate information from such systems is likely to be significant. Such consequences can occur as a result of a variety of threats as well, including manmade deliberate and manmade unintentional. Manmade deliberate threats can include individuals who want to cause confusion or mayhem, and they may elect to perform their attack(s) during other incidents—to leverage it as a "force multiplier" of their own attack.

Manmade Unintentional Threat—Emergency Management

Unintentional threats can also cause such an incident, which would most likely occur as a consequence of carelessness or fatigue and result in an accidental release of inaccurate information. Unintentional releases of such information could be detected immediately, for example, by a Joint Information Center), while deliberate attacks might not be as easy to detect because the deliberate actor may not want to be detected in the process of conducting the attack.

The vulnerabilities or enablers of a release of inaccurate or false information via an alerting and warning system could occur for a variety of reasons, mostly related to human and process vulnerabilities. Public announcements typically are vetted through an approval process that seeks to minimize the potential for release of false or inaccurate information. These procedures usually include review of the materials by more than one individual to ensure the accuracy of its content. In addition, these procedures can vary across various media. For instance, an EAS, which has been in use for several years, may have very mature and tested procedures. However, new technologies, such as online social media services, which have large user bases, have increasingly become useful tools to emergency management agencies because they are inexpensive to manage and maintain, and the users can easily gain access to notifications from their local emergency management or emergency services entity/entities. The procedures for vetting information that goes out on these newer technologies are typically spontaneous in nature or do not readily allow for compliance with long-established processes. New technologies—because of their emphasis on having user-friendly interfaces—can also lend themselves to simple

[11] An example of this is a Reverse 9-1-1 system, which can be used to rapidly dial the home and business telephones in a defined segment of a community, an entire community, or even an entire jurisdiction to issue warnings such as "Boil Water Orders" when a major public water distribution failure has occurred. Local, State, Federal, and tribal emergency management agencies have some level of access to EAS, whether it is with local television or radio broadcast stations or satellite and cable communications companies, or more.

mistakes, such as an individual accidentally sending out a personal message to the emergency management agency's official account.[12]

Impacts of social media mishaps have historically resulted in embarrassment to the entity whose account was mistakenly used. For other alerting and warning systems, though, the public dissemination of inaccurate or incorrect information regarding a real or perceived incident could have a significant impact on local jurisdictions and their citizenry. The most immediate impact, unless the error is immediately detected, is that organizations and individuals can begin mobilizing or reacting to the information in ways that affect the community, including reallocation of emergency response, law enforcement, and fire and emergency services personnel and resources, which would divert their limited resources from potentially legitimate and more urgent incidents or emergencies.

To manage the risks associated with a deliberate or unintentional release of inaccurate or false information from an alerting and warning systems, ESS entities should account for the tools and technologies that they use for the public release and notifications of incidents and ensure that timely and sufficient policies and procedures are in place to manage the posting and release of information through them. Furthermore, the emergency management discipline and ESS entities in general should practice basic cybersecurity measures on a regular basis, while also identifying unique security enhancements that are necessary to manage the appropriate release of information through alerting and warning systems (e.g. regularly changing passwords and establishing complex passwords).

4.6. Scenario 5: Loss of Communications Lines Results in Disrupted Communications Capabilities

Scenario 5 focuses on loss as a result of manmade deliberate and manmade unintentional threats to all ESS-related communications. This scenario expands the scope of Scenario 1. The components of Scenario 5 include undesired consequences, the vulnerabilities that can lead to those undesired consequences, and the threats that can exploit those vulnerabilities. The components are relevant to all ESS disciplines but focus on EMS, public works, and PSC&C disciplines. The consequences, vulnerabilities, and threats were identified in elicitation sessions with ESS stakeholders. Figure 24 depicts the relationships among the consequences, vulnerabilities, and threats in the scenario.

[12] For an example of mistaken use of a corporate social media account instead of a personal one, see: http://money.cnn.com/2011/02/17/smallbusiness/dogfish_redcross/index.htm. Accessed on 2/2/2012.

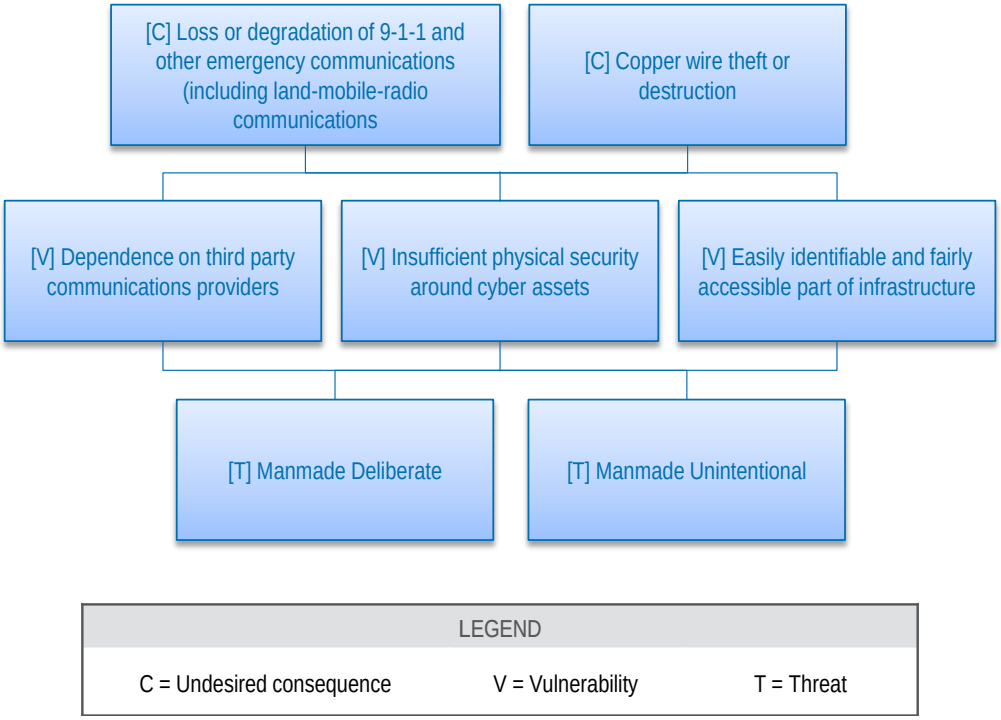

Figure 24: Scenario 5 Consequences, Vulnerabilities, and Threats

Loss of communications is one of the most difficult scenarios that ESS faces. As shown in Figure 25, every discipline, all elements of the value chain, and a majority of the supporting cyber infrastructure can be affected. As the ability to communicate is foundational to many pieces of the supporting cyber infrastructure, when communications systems fail, situational awareness for law enforcement officers, firefighters, EMS providers, emergency managers, public works specialists, and the general public can be severely degraded. Depending on the exact nature of the situation, all parties will have to use less efficient and effective *ad hoc* communications methods, such as public broadcasting, door-to-door notification, and word of mouth.

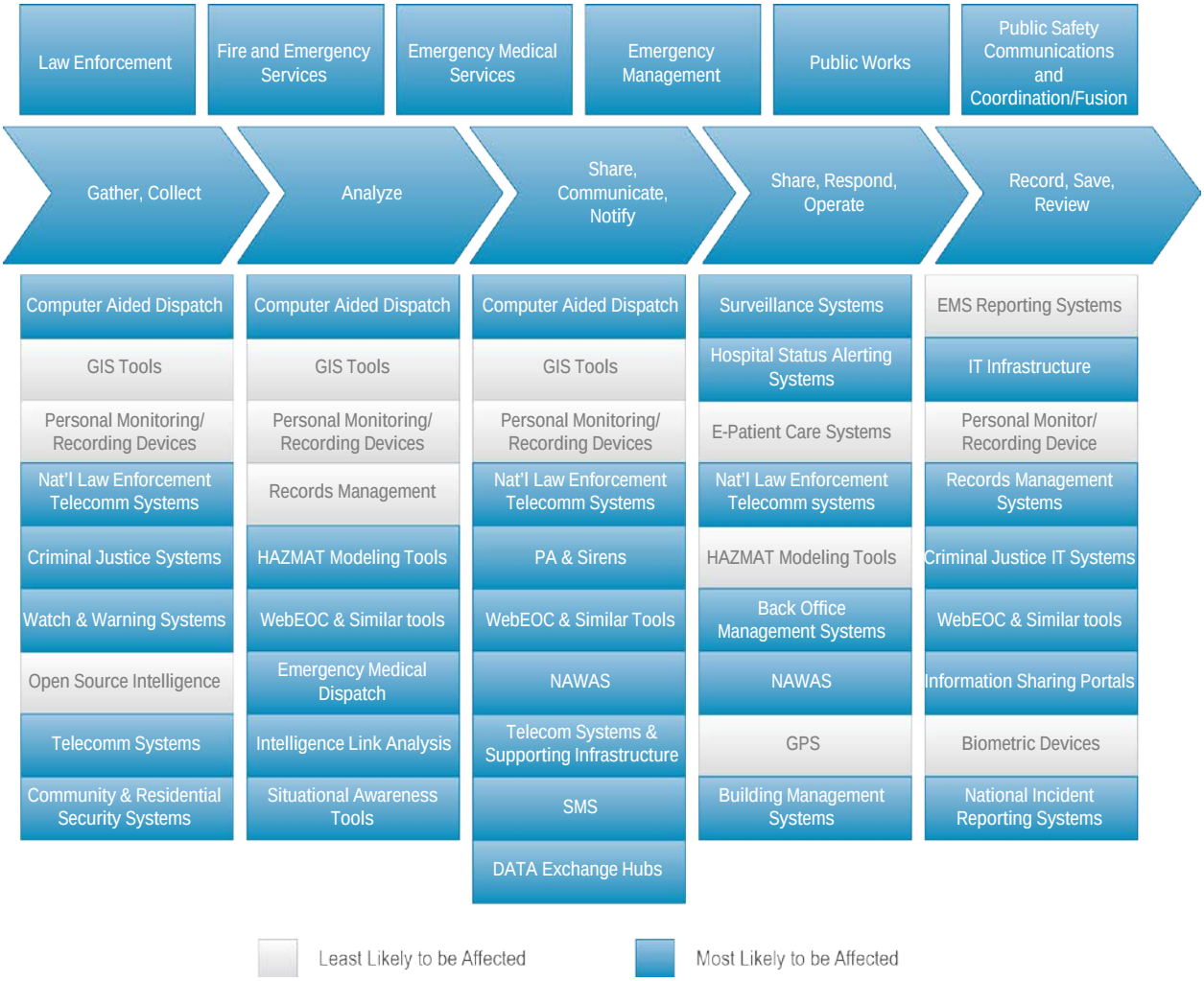

Figure 25: Scenario 5—Disciplines and Cyber Infrastructure Affected

Risk Assessment Scenario 5: Loss of Communications Lines Results in Disrupted Communications Capabilities

Figure 26 shows that in the case of a manmade deliberate threat in this scenario, the relative consequence is generally high and the likelihood of the threat is generally low, though medium specifically for fire and emergency services discipline. The ESS disciplines affected in this scenario will encounter roughly similar consequences depending on the specific communications lines lost.

Figure 26: Relative Risk Profile of Scenario 5: Loss of Communications Lines Results in Disrupted Communications Capabilities—Manmade Deliberate

For a manmade unintentional threat, the likelihood of the scenario is slightly higher for some disciplines but the consequences generally are lower as shown in Figure 27. The likelihood will be slightly higher because there are a significant number of construction workers and other individuals who could potentially interfere with communication lines through carelessness and lack of awareness. The PSC&C, fire and emergency services, and EMS disciplines are especially affected in this case. The consequence will likely be slightly lower because mistakes may tend to be more minor because unintentional threat actors usually attempt to adhere to policy that prevents the scenario.

Figure 27: Relative Risk Profile of Scenario 5: Loss of Communications Lines Results in Disrupted Communications Capabilities—Manmade Unintentional

Manmade Deliberate Threat—Fire and Emergency Services

Deliberate acts that cause the loss of communications lines include the theft of copper wire from radio frequency (RF) infrastructure sites, eliminating the antenna connectivity and/or the power supplies needed to support RF equipment and, in many cases, to carry radio traffic. These acts also include, but are not limited to, the theft of RF infrastructure components and vandalism to RF infrastructure sites. The result of these acts may not cause a widespread communications failure but are capable of causing local failures. The cumulative effect of a high number of such thefts and vandalism has made this a national-level threat.

As a consequence of such deliberate acts, fire and emergency services personnel may partially or completely lose connectivity between units or with dispatchers. Full or partial disruptions jeopardize the health and safety of firefighters, HAZMAT response teams, and others delivering service in this discipline because they may be unable to notify incident commanders when they

urgently need additional resources or when they are lost, disoriented, or trapped in an environment that presents an immediate danger to life and health. These disruptions also jeopardize the general public because they may delay the deployment of firefighters to burning buildings or to HAZMAT spills. Law enforcement personnel may also partially or completely lose connectivity with other units or with dispatchers. Such disruptions can decrease officer safety, because they lose situational awareness of complaint responses, traffic stops, and suspicious persons and events that other officers are encountering. This may delay backup when it is most needed, which could place officers in the position of using greater force to overcome a threat to themselves or to the public than would be otherwise necessary, if additional units were on the scene. Law enforcement officers encountering high-risk situations may be at greater risk of bodily harm if they cannot communicate with other officers or their dispatchers.

The greatest threat to the RF infrastructure from deliberate acts today lies with thieves. Scrap metal prices are at record highs because society has placed a high value on recycling metals rather than creating them from raw materials and the cost to accomplish this and distribute recycled materials of high quality and quantity has reached commercially viable levels. Copper has been a particularly lucrative metal seen at scrap facilities, where prices on a November day in 2011 were seen to average between $3.09 and $3.34 per pound, depending on the quality of the copper presented, an increase in value of 79% from the week before, according to one scrap metal Web site.[13] This sort of market makes taking the risks of discovery, prosecution, or even electrocution, acceptable to thieves. One such example of the extreme risks that thieves are willing to take occurred in Dallas, Texas, in March 2010, when a group of young men were electrocuted and burned to death when they attempted to steal an energized (13,200 Volts Alternating Current) copper line.

There are a few key vulnerabilities associated with these threats:

- **Insufficient physical security around cyber assets.** Many RF sites for land mobile radio (LMR) systems are located in remote areas based on coverage requirements. Therefore, they may be atop a mountain or perched on poles in a large field to carry signal between dispatchers and field forces. Some sites are located on private property, where agencies providing LMR services may not have the ability to erect the physical barriers they may need. Others may have limited barriers, such as simple fence lines, without any supporting services such as guards, surveillance cameras, or alarm systems because of limited power supplies or connectivity.
- **Easily identifiable and fairly accessible part of infrastructure.** Copper wire, even when it is insulated, is easy to identify. Even thieves with limited experience with wire or electrical systems can easily discern copper wire at connection points. Often, copper lines are connected to RF infrastructure outdoors or in areas where it is obvious that copper resources are being used, such as along radio tower components.
- **Dependence on third-party communications providers.** Many agencies use commercial service providers to erect, maintain, and/or repair their LMR systems because it may be more economical than operating an internally staffed and equipped radio shop. Under such circumstances, it is more difficult to determine whether these

[13] Based on prices quoted for the last date posted—11/23/2011, http://www.scrapmonster.com/. Accessed on 12/2/2011.

providers are exercising sufficient security measures to assure that their staff members are provided with effective security policies and guidelines, are well trained, are trustworthy, and are reliable when servicing and protecting these systems, or whether they have implemented and maintained security measures that provide adequate protection for the infrastructure for which they care.

The general risk in this scenario indicates a moderately low likelihood that such deliberate acts will occur to any given fire and emergency services communications network. Rural agencies may face greater likelihood because their RF sites may have less physical security available; in suburban and urban areas, these sites are generally in areas within public view and have greater physical security measures protecting them. Nonetheless, the consequences of such deliberate acts can be equally grave, and present the highest risk if they occur.

Although the deliberate act presents the greatest threat to communications line in either their "first mile" or "last mile" (i.e., when they are most visible to thieves and when their connections to critical infrastructure are most apparent), the unintentional loss of these lines almost always occurs when the lines are not visible. It is when the presence of communications lines is not known because they are buried, or because they are "out of sight and out of mind" when they are carried overhead. It is when the RF site components to which they are connected may not be recognized or understood for the essential support they provide because they are hidden away in a closet or they appear to be part of other electronic applications, such as computers or telephony. Likewise, telephone lines that support LMR communications may not be recognized when bundled with regular telephone service landlines. This relative invisibility creates the risk of an unintentional loss of local communications lines.

Manmade Unintentional Threat—Emergency Medical Services

Accidental disruptions may occur in a variety of circumstances. When the telephone lines connecting LMR sites with emergency communications centers are collocated with other telephone lines, they may be prone to accidental interruptions when disconnections, relocations, or other legitimate and planned outages may otherwise be taking place. Construction projects and utility work for other interests create risk for these lines because such activities rely on accurate depictions on maps and well-placed ground markers and utility flags to avoid accidentally severing such lines while using earthmoving equipment. Disruption can be caused by something as simple as an incorrectly placed shovel or as complex as a backhoe striking a cable bundle in which communications lines are trunked or collocated with dozens, or perhaps even hundreds, of other lines. Communications lines can also be lost when critical RF components fail or are incorrectly manipulated. If a Base Interface Module (BIM) fails because of a defect, a critical RF component fails because it has reached the end of its life cycle, or if a dispatcher accidentally disables a repeater site from his or her radio console, the resulting disruptions to emergency communications are the same. While these disruptions can affect any ESS discipline, EMS providers may be particularly affected by accidental disruptions. The high volume of emergency calls to which this discipline responds requires reliable LMR communications to transmit and receive dispatches, make hospital notifications, seek on-line medical direction, and assure that the proper level of care providers are routed to the incidents for which their skills may be best suited.

The time to make repairs or corrections will vary widely in these various accidental disruptions. The accidental command or erroneous manipulation of controls can be quickly detected and corrected. If a BIM card fails, as long as a replacement or spare is readily available, the problem can be resolved in minutes if someone is available that is trained to recognize and troubleshoot that problem. The loss of communications lines somewhere between that first and last mile of connectivity is a much more difficult problem. It can take hours to locate the source of such trouble, depending on the cause, and hours to days to make repairs, depending on how many lines in the affected cable bundle were severed.

There are a few key vulnerabilities associated with these threats:

- **Insufficient physical security around cyber assets.** As noted before, the ability to secure emergency communications infrastructure presents a significant vulnerability that can be easily exploited, even if done so accidentally or unintentionally. In the latter circumstance, it is the collocation of communications lines with other lines not used by ESS that presents vulnerability to accidental disruption. It is difficult, if not impractical, to protect miles of telephone lines leased to ESS organizations from the effects of weather, deterioration, or cutting in a manner separate from regular commercial or residential communications lines.
- **Human factors may present unanticipated vulnerabilities resulting from accidents.** Whether the people who may accidentally cause the loss of a communications line are part of an ESS organization or not, the interaction of people and their activities in proximity to essential communications lines is ever-present. Construction projects or utility repairs occur across the country on most weekdays. Equipment operators may be well trained, but if the presence of underground utilities has not been determined, or if the markers, such as flags, have been altered by passersby or others, their earthmoving equipment can easily inflict permanent or long-term damage in a matter of moments. Communications staff, whether they are dispatchers or technicians, can accidentally disrupt these lines with errors in commands or by performing other acts that unwittingly disconnect lines, such as cleaning activities, moving equipment, or shutting off unrelated equipment.
- **Variance in capabilities of the third-party providers to address communications disruptions.** In most instances across the country, ESS must rely on commercial service providers for the connectivity among their proprietary LMR systems terminal points, such as RF sites, communications centers, and broadcast towers. There are alternatives available such as microwave, to carry signals between RF sites, but in the end, a telephone is still a line used to carry that signal to the dispatch console or to the broadcast antenna. The ability of a commercial service provider to detect and repair a disruption can vary widely, based on factors such as technician availability, the age and condition of the infrastructure, the weather, and even time of day or day of week if a disruption occurs after regular business hours.

Manmade Unintentional Threat—Public Safety Communications and Coordination/Fusion

There could be a number of impacts of degraded emergency communications capabilities. These impacts include—

- Inefficient or ineffective allocation of resources during an incident
- Longer dispatch and response times because of a lack of real-time or near-real-time situational awareness of people, resources, and emergencies
- Incomplete or lack of alerting and warning capabilities used to indicate or announce emergencies to the general public.

These consequences can cascade into loss of life, loss of economic security, impacts on healthcare and public health services, and widespread loss of confidence in government, its services, or its messages to the public.

Telecommunications networks and infrastructure are critical to the PSC&C discipline, because first responders and public safety communications agencies use a variety of communications services, from POTS to cellular telephones and smartphones, pagers, and personal digital assistants (PDA). These services help public safety agencies receive and process calls, analyze location data about callers, and make notifications to allied services (e.g., law enforcement, fire and rescue, public utilities). Public safety radio networks (such as LMR and radios in the aviation and marine bands that engage in patrol, response, search, rescue, and evacuation operations) use telecommunications networks for backhaul services. In addition, reliance on telecommunications services is increasing steadily as more and more public safety agencies transition from legacy analog services.

The primary threats that could cause this scenario are manmade unintentional threat actors who could accidentally damage or sever communications lines.[14] These include employees, third-party contractors, construction workers, maintenance workers, and telecommunications service workers. With each of these actors, the action could be caused by carelessness/recklessness (e.g., not coordinating with utility location services to understand where communications lines are located before starting construction), a lack of training, or a technical flaw. The vulnerabilities include a lack of route diversity, aging infrastructure that is not well protected, mismarked utility markings, or a lack of attention paid to utility markings. Overall, the likelihood of these threats exploiting one of these vulnerabilities was determined to be low to medium.

Direct consequences of this scenario to ESS in general and the PSC&C discipline in particular may include the loss of the HPH Sector's ability to provide adequate care and emergency response. With dependence of all ESS disciplines on the PSC&C discipline, the consequences were assessed to be medium to high, depending on the severity and length of the outage. The impact of this scenario is likely to be felt more strongly on a local scale. At a regional level or higher, there is significantly more redundancy and route diversity built into the network, resulting in greater failover capabilities, resilience, and service continuity. Moreover, the consequences of this scenario may be mitigated on even a local level by increased route diversity or better access controls. However, it is important to note that in this scenario, recovery and reconstitution of the network depends primarily on third-party communications service providers and are therefore largely out of the control of public safety agencies. This also means that public

[14] It should also be noted that while this scenario focuses on the manmade deliberate or unintentional threats to communications lines, natural disasters can also cause the same or similar effects as those expressed in this scenario's analysis. Since natural disasters are specifically discussed in Scenario 1, the participants did not evaluate the impact of a natural disaster on physical communications lines.

safety organizations have fewer options to directly mitigate or reduce key vulnerabilities that could cause this scenario. Furthermore, while the impact may be felt only at a local level, it may put significant strain on local public safety resources.

4.7. Scenario 6: Closed-Circuit Television Jamming/Blocking Results in Disrupted Surveillance Capabilities

Closed-Circuit Television (CCTV) jamming/blocking that results in disrupted surveillance capabilities would most likely affect the public works, emergency management, and law enforcement disciplines. Many CCTV networks are switching to IP-based communications, creating new vulnerabilities for threat actors to exploit. Older CCTV networks are also prone to attacks from various threats. Potential consequences from CCTV jamming/blocking include the inability of law enforcement personnel to apprehend criminals, difficulties for emergency management personnel trying to identify where to allocate resources, potential public panic or chaos if traffic systems are affected, and disruption to public works' ability to monitor and/or respond to incidents. The components of this scenario include undesired consequences, the vulnerabilities that can lead to those undesired consequences, and the threats that can exploit those vulnerabilities. The components are relevant to the following ESS disciplines: law enforcement, EMS, emergency management, and public works. The consequences, vulnerabilities, and threats were identified in elicitation sessions with ESS stakeholders. Figure 28 depicts the relationship among the consequences, vulnerabilities, and threats in the scenario.

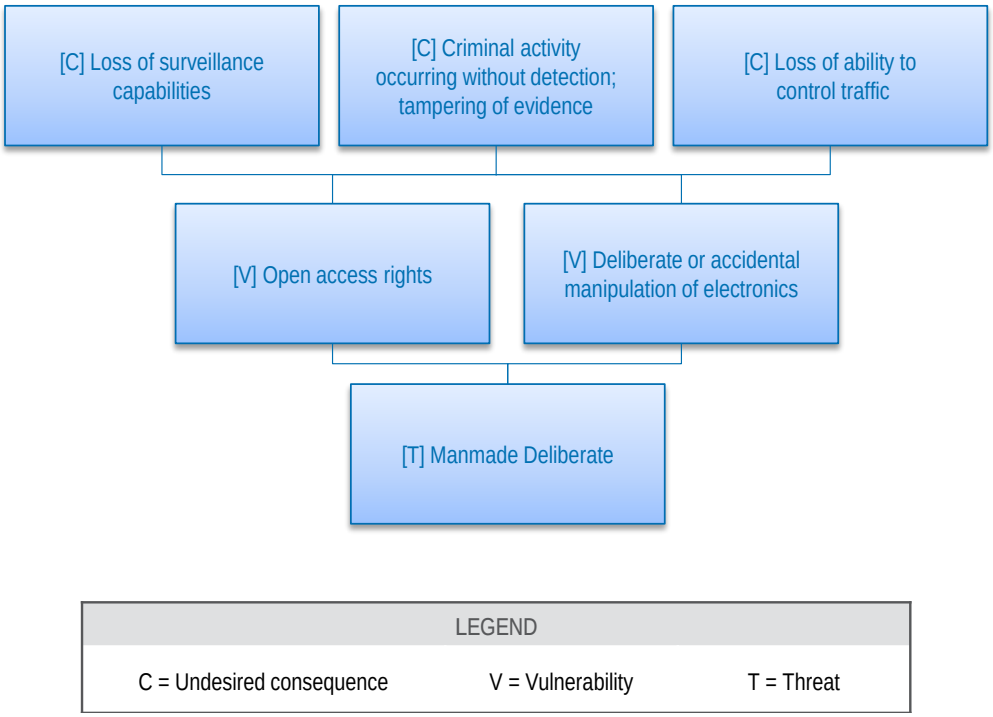

Figure 28: Scenario 6 Consequences, Vulnerabilities, and Threats

Figure 29: Scenario 6—Disciplines and Cyber Infrastructure Affected

In the past decade, CCTV has evolved into a highly efficient and effective public safety tool used to deter crime, monitor critical assets, and provide the technology to manage public safety responses in real time. As shown in Figure 29, when CCTV is jammed or blocked, law enforcement and emergency managers lose their "eyes and ears," thereby degrading their ability to monitor critical assets (e.g. buildings, power plants, roads, airports, bridges) as well as monitor and manage public safety events. In these types of situations, monitoring and surveillance may need to be performed by placing law enforcement officers physically onsite.

Risk Assessment Scenario 6: Closed Circuit Television Jamming/Blocking Results in Disrupted Surveillance Capabilities

Figure 30 shows that in the case of a manmade deliberate threat in this scenario, the likelihood of the threat affecting the ESS disciplines is low to medium and the relative consequences range from high for public works, medium for emergency management and law enforcement, and low for EMS. The public works discipline in general will be highly affected because of its need to

monitor locations to accomplish its mission. Due to the scope of consequences for this scenario is mostly local, the target of the manmade deliberate threat will cause the relative consequence to the disciplines to vary.

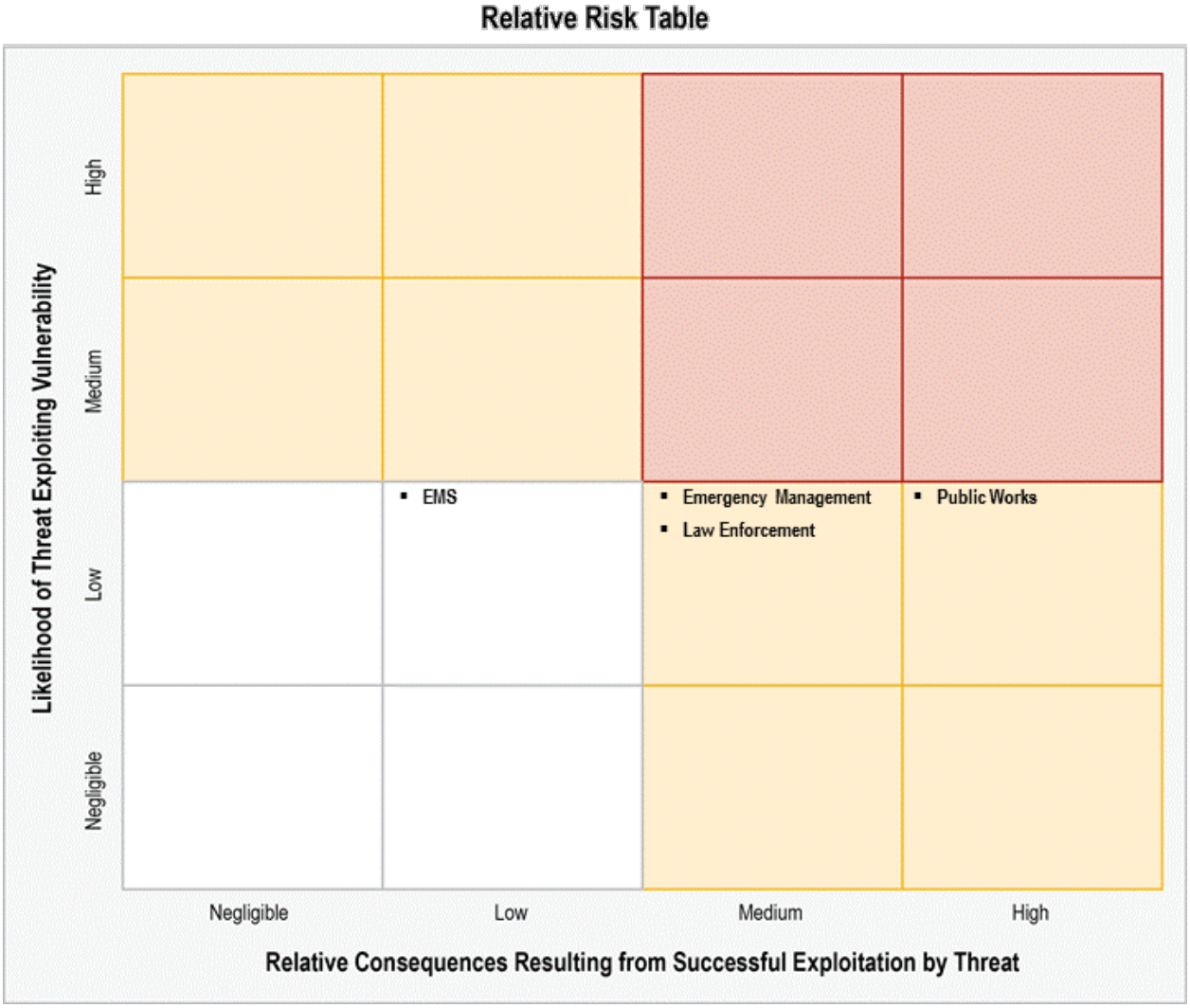

Figure 30: Relative Risk Profile of Scenario 6: Closed Circuit Television Jamming/Blocking Results in Disrupted Surveillance Capabilities—Manmade Deliberate

Manmade Deliberate Threat—Public Works

The jamming or blocking of CCTV systems hinders the public works discipline's ability to monitor critical infrastructure facilities and systems or high-risk infrastructure areas. The inability to monitor these facilities and areas impedes public works agencies from detecting and preventing physical incidents. The situational awareness provided by CCTV also assists ESS in responding to and recovering from physical incidents such as motor vehicle collisions or disabled vehicles blocking traffic. In the event of a jammed or blocked CCTV, this response could be delayed. Other potential incidents monitored by CCTV cameras include debris blockages in wastewater processing systems or mechanical failures in other environmental

systems. The general public will likely be affected through increased traffic congestion or possibly through the disruption of utility services. The effects of a jammed or blocked CCTV system could cascade to other sectors, including the Dams, Water, and Transportation Systems Sectors, which have close ties at the local level to the public works discipline.

Cyber vandals are the typical threat actors associated with this type of incident, although any actor with a physical component to its objectives may attempt to jam or block a CCTV system to mask its activities. Cyber vandals often target CCTV systems for their own amusement or to cause embarrassment to public works officials. These types of attacks require minimal funding and are often crimes of opportunity rather than intricately planned endeavors. In most cases, tools, such as signal jammers, are required but are readily available and easily adapted to fit the actor's needs. These types of actors often seek to keep their identities hidden and rarely commit more than minor criminal acts, such as vandalism or trespassing. In addition, actors often must gain physical or logical access to the CCTV system, which increases the difficulty of jamming or blocking the system. Physical security measures and placing cameras out of reach further constrain an actor's ability to gain physical access to the system, and system monitoring and access controls can constrain logical access to the system. Enhanced redundancy measures, such as employing multiple cameras, reduces the overall risk posed by a jammed or blocked CCTV system.

Several vulnerabilities exist within the people, processes, and technology associated with CCTV systems that can be exploited by threat actors to jam or block the system. CCTV control stations placed in public spaces increases the time a threat actor has to access the system. Employees may knowingly or unknowingly disclose the location of control stations or cameras to threat actors, or even execute commands on behalf of the threat actor. In some cases, these vulnerabilities are introduced as a result of inadequate clearance checks and employee vetting, a lack of operational security, or a lack of communications security related to CCTV system use. The technology itself is vulnerable to exploitation, and the move to IP-based systems provides threat actors with the ability to use cyber exploits to jam or block CCTV systems and retrieve or manipulate the audio and video recordings stored on those systems. Measures currently employed by public works agencies to address these types of vulnerabilities include placing control stations in secured facilities, performing rigorous employee vetting and training, and implementing industry standards and guidelines for the management of CCTV systems.

The jamming or blocking of a CCTV system would lead to significant undesired consequences for the Public Works discipline. However, there is low likelihood that this type of incident will occur because of the risk responses currently employed by the discipline. In the future, risks to the discipline's CCTV systems could change or increase as public works agencies move to IP-based CCTV systems.

4.8. Scenario 7: Overloaded Communications Network Results in Denial of Service Conditions for Public Safety and Emergency Services Communications Networks

This scenario specifically focuses on the loss of availability of PSC&C networks as a result of denial of service conditions. This scenario can occur deliberately as a result of a malicious actor launching a denial of service attack or unintentionally as a result of a network overload caused by a sudden and unexpected surge in public use.

In addition to affecting wireless communications networks, this scenario is applicable to Next-Generation 9-1-1, IP-based, and other cloud-based communications networks, which are also vulnerable to manmade deliberate and unintentional threats and are of increasing importance in ESS.

The components of this scenario include undesired consequences, the vulnerabilities that can lead to those undesired consequences, and the threats that can exploit those vulnerabilities. The components are relevant to all ESS disciplines but focus on the law enforcement, fire and emergency services, EMS, and PSC&C disciplines. The consequences, vulnerabilities, and threats were identified in elicitation sessions with ESS stakeholders. Figure 31 depicts the relationship among the consequences, vulnerabilities, and threats in the scenario.

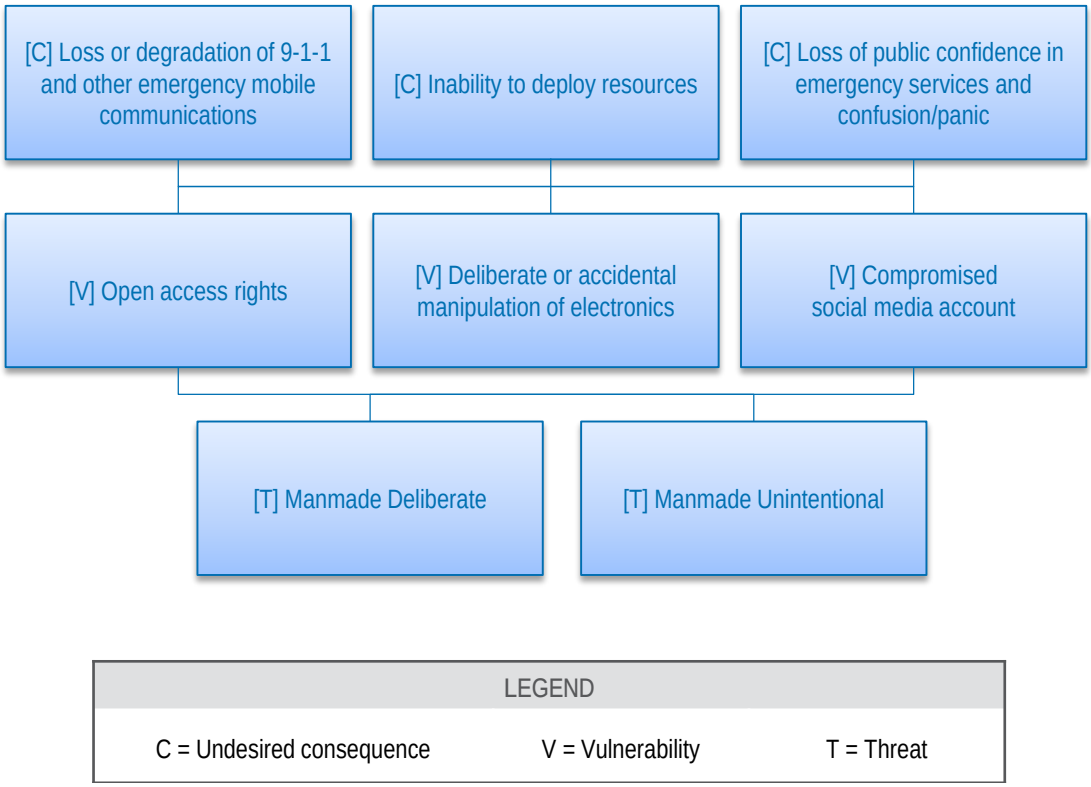

Figure 31: Scenario 7 Consequences, Vulnerabilities, and Threats

As shown in Figure 32, an overloaded communications system or network that results in a denial of service could affect multiple disciplines, segments of the value chain, and numerous supporting cyber infrastructure components, particularly those components that are IP-based. In this scenario, situational awareness tools such as CAD and GIS tools could be negatively affected across the value chain, potentially resulting in a life-threatening delay of service to customers. In the worst cases, typical ESS services would be unavailable to customers until the issues were resolved. 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 the system is unresponsive or slow to respond, causing potential loss of life and damage to property.

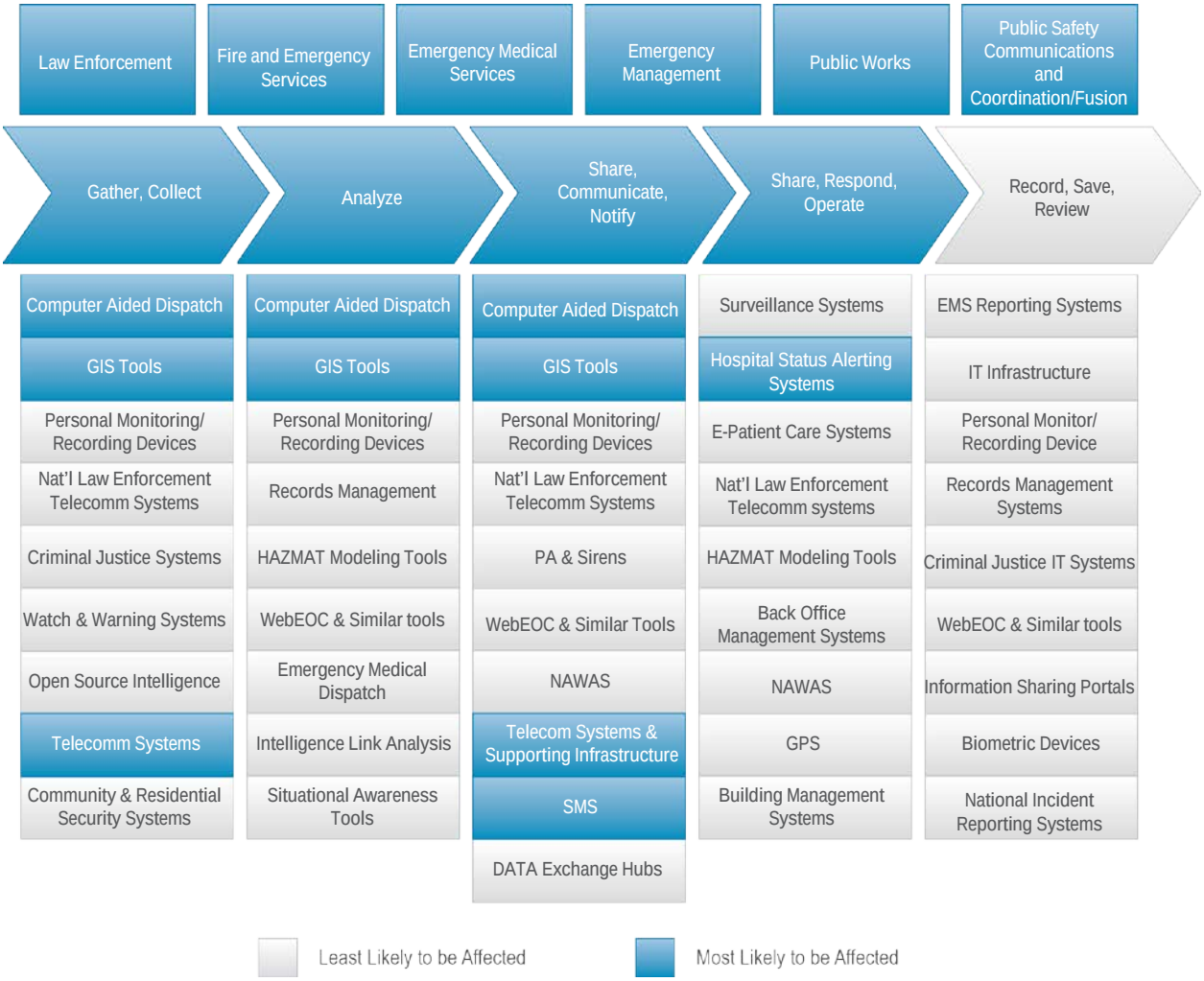

Figure 32: Scenario 7—Disciplines and Cyber Infrastructure Affected

Risk Assessment Scenario 7: Overloaded Communications Network Results in Denial of Service Conditions for Public Safety and Emergency Services Communications Networks

Figure 32 indicates that this scenario affects all the ESS disciplines. In the case of a manmade deliberate threat in this scenario, the likelihood of the threat affecting the ESS disciplines is low but the consequences for all disciplines are medium to high. The likelihood is low because of the effort level associated with deliberately triggering the scenario. A manmade deliberate actor would need to focus significant resources on one location over a period of time to successfully execute this scenario. However, given the increasing strength of botnets (a collection of

compromised computers connected to the Internet) available to hackers, this attack may be more feasible, especially for localized areas, in the near future.[15]

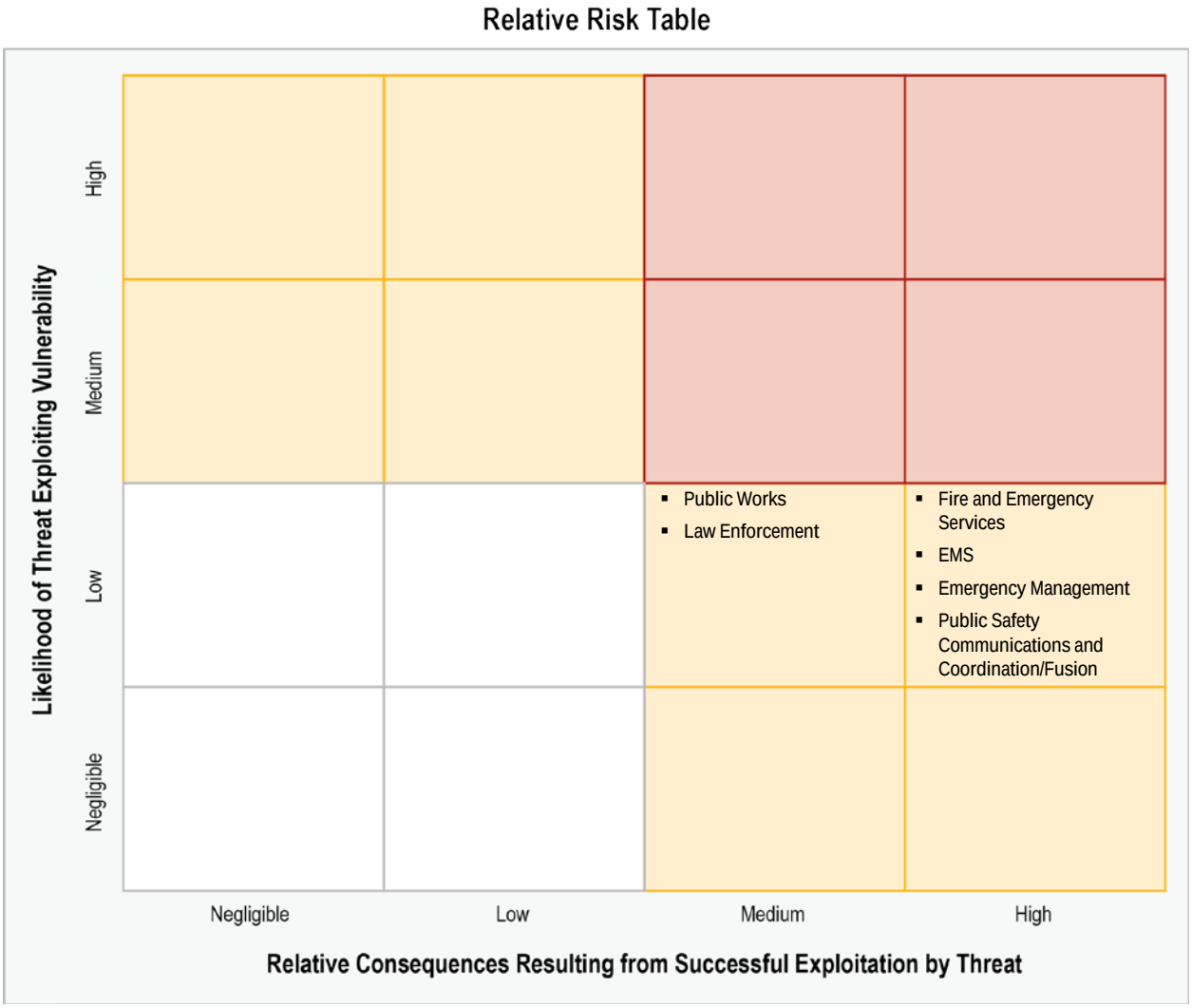

Figure 33: Relative Risk Profile of Scenario 7: Overloaded Communications Network Results in Denial of Service Conditions for Public Safety and Emergency Services Communications Networks—Manmade Deliberate

For the manmade unintentional threat, the likelihood for the fire and emergency services and EMS disciplines increases to medium as shown in Figure 33. An example of a common manmade unintentional threat for this scenario would be a large event or gathering. The large event or gathering would result in a large volume across local communications networks thus creating an unintentional distributed denial of service.

[15] The Federal Communications Commission Communications Security, Reliability, and Interoperability Council III has a working group dedicated to developing recommendations and guidance for botnet remediation. (http://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-council-iii. Accessed on 2/5/2012).

Figure 34: Relative Risk Profile of Scenario 7: Overloaded Communications Network Results in Denial Of Service Conditions for Public Safety and Emergency Services Communications Networks—Manmade Unintentional

Manmade Deliberate Threat—Emergency Medical Services and Fire and Emergency Services

EMS and fire and emergency services agencies use a variety of wireless cyber resources across the country. Many wireless networks are being adopted for use in supporting emergency, non-emergency, and administrative communications requirements for voice, data, and in some cases, video services. In most parts of the country, emergency communications are conducted using proprietary LMR networks and dedicated private lines for landline connectivity between communications centers and hospitals, aeromedical evacuation services, law enforcement, or fire and emergency services agencies. When other wireless services are used, they are generally the same services used by the average American consumer—Enhanced Special Mobile Radio (ESMR), cellular telephones, short message services, and data. When the demands for service by ESS and the public peak simultaneously, the networks supporting these commonly accessible services are overloaded. The result is that communications can deteriorate significantly.

Major emergencies, such as the terrorist attacks of September 11, 2001, have proven that even in urban areas in which commercial communications services are robust and built to serve hundreds of thousands of call requests in a short period of time, the availability of these systems can be lost in less than an hour. On August 23, 2011, a moderate earthquake centered near Mineral, Virginia, generated a huge demand for wireless communications access in just a few moments. The available infrastructure was unable to support these demands and resulted in busy signals or lost calls in less than 10 minutes in such population centers as Washington, D.C.—more than 90 miles from the epicenter of the quake. A government program designed to provide access to critical end users in government and emergency services, the Wireless Priority Service, failed to support authorized subscribers on any commercial systems.[16]

When a surge in demands can be predicted, commercial service providers can prepare by placing extra temporary infrastructure into position. For example, in 2009, the District of Columbia Homeland Security and Emergency Management Agency developed a Presidential Inauguration Communications Plan in which it made assumptions about record demands for wireless communications services as more than one million Americans were believed to be planning to attend the historic inauguration of the country's first African-American president. The agency worked with commercial communications providers to address their concerns. In a regional after action discussion, National Capitol Region ESS representatives noted that three major service providers placed Cell on Wheels and Cell on Light Truck units at a number of downtown locations, an action that proved itself invaluable as demands spiked at more than 1,000 times greater than normal while Barack Obama took his Oath of Office. In the vicinity of the National Mall, people attending the event sent text messages, held their mobile telephones with open lines to loud speakers, or sent photos to share their experience with others who could not be there. Although many people experienced dropped calls, or were denied access to their networks because of the volume in demand, the systems did not crash. More important, in that instance, the WPS worked when its subscribers, including local fire and emergency services officials, were unable to complete calls using conventional dialing.

Given the examples discussed here, it is apparent that any incident that creates a widespread concern among the public and a subsequent surge in demand for wireless communications access can create an overloaded network. The ability to predict such surges, such as for scheduled events, provides commercial service providers with an opportunity to apply temporary infrastructure to help meet that surge. It is when the unpredictable event or emergency incident occurs that an overloaded network presents the greatest threat to ESS.

[16] As reported by the online magazine, *NextGov*, available on the web at http://www.nextgov.com/nextgov/ng_20111128_2122.php?oref=search. Accessed on 12/12/2011.

There seem to be three major consequences for EMS agencies when wireless communications networks are overloaded.

- **Loss or degradation of 9-1-1 and other emergency mobile communications.** EMS organizations may use such commercial services such as ESMR to coordinate activities with other government agencies serving in their area, or to conduct administrative communications with communications centers or firehouses. They may use cellular telephones to communicate with outside resources such as language line services, CHEMTREC®[17], poison control, or online medical control when they require subject matter expertise to effectively manage a response problem. EMS may use cellular telephones to obtain authorization to implement medical interventions that exceed standard protocol to save a seriously ill or injured patient. As the public is competing for access to these same commercial networks, callers may experience degraded abilities to call for help because they are unable to complete or lose calls placed to 9-1-1 centers that support the EMS and fire and emergency services agencies.
- **Inability to deploy resources effectively.** Although the EMS discipline may not use commercial wireless networks for emergency communications (e.g. LMR support) it may use commercial networks to support key resources such as mobile data networks used to dispatch and deploy field forces, jurisdiction-specific navigational aids, or access to information services such as online medical libraries or building pre-plans. This can cause delays or lost assignments, or lost access to key medical information at a time when lives may be at stake.
- **Loss of public confidence in emergency services and confusion/panic.** When one is in dire need of EMS or fire and emergency services, the ability to acquire dial tone and complete a call to 9-1-1 or other emergency telephone number is essential. When callers cannot reach anyone by dialing an emergency number, it creates doubt about the effectiveness of the response system. People become confused because they may not be aware of other numbers to dial for help, or they may panic because they do not know how to summon the help they need. Many people, especially travelers, have no idea at a given time where the nearest hospital, rescue squad, or fire station to their location may be, and so they cannot even make a personal report of an emergency to get help started.

Fortunately, the likelihood of an emergency significant enough in scope to create an overloaded network is low for any given EMS or fire and emergency services agency. Although there are hundreds of thousands of emergencies that these disciplines respond to every day, the number of those incidents that escalate to create such surges are very few; therefore, while the likelihood is low, the consequences should such an incident occur are very high.

[17] CHEMTREC is the Chemical Transportation Emergency Center, a service of the American Chemistry Council. CHEMTREC was established as a hotline for emergency responders, such as firefighters, HAZMAT emergency response teams, and law enforcement, to obtain information and assistance for emergency incidents involving chemicals and hazardous materials.

5. EMERGENCY SERVICES SECTOR CYBER RISK ASSESSMENT KEY FINDINGS AND NEXT STEPS

5.1. Emergency Services Sector Cyber Risk Assessment Key Findings

The ESS-CRA found that all evaluated ESS disciplines are vulnerable to a variety of manmade deliberate, manmade unintentional, and natural threats to their cyber infrastructure. These threats to ESS can occur in a variety of forms. Manmade deliberate threat actors can include disgruntled insiders, criminals, protestors, and hacktivists. Manmade unintentional threats can stem from inadequately trained employees misusing software, technical flaws, or lack of oversight enabling incidents to occur as a result of employee errors. Natural threats affecting ESS can consist of biological threats (e.g., epidemics), geological threats (e.g., earthquakes), or meteorological threats (e.g., floods). The likelihood of these threats causing an incident increases when paired with common vulnerabilities such as weak security policies and procedures, poorly secured technology and software, or inadequate security architectures.

Using DHS/ NCSD's CARMA, ESS stakeholders developed scenarios and applied them across sector disciplines. These scenarios consisted of threat, vulnerabilities, and consequences that highlighted the specific risks posed to ESS cyber infrastructure. ESS stakeholders identified specific risks in a collaborative and iterative process that consisted of risk analysis and evaluation. Table 8 includes high-consequence and high-likelihood cyber risks for each discipline, as well as potential impacts.

Table 8: High-Consequence and High-Likelihood Cyber Risks to Emergency Services Sector

Law Enforcement	
Risk	*Operational Impacts*
Natural disaster causes loss of 9-1-1 capabilities	• Unavailability of certain critical systems; possible inability to coordinate incident response or stay notified of incidents • Reduced response coordination effectiveness
Loss of communications lines as a result of an unintentional or deliberate threat results in disrupted communications capabilities	• Loss or degradation of 9-1-1 services • Compromised responder safety compromised
Public alerting and warning system disseminates inaccurate information as a result of an unintentional or deliberate threat	• Redirection of first responders to false alarms/ wasting resources • Public confusion and panic

Fire and Emergency Services	
Risk	*Operational Impacts*
Natural disaster causes loss of 9-1-1 capabilities	• Unavailability of certain critical systems; possible inability to coordinate incident response or stay notified of incidents • Reduced effectiveness of element coordination
Loss of communications lines as a result of an unintentional or deliberate threat results in disrupted communications capabilities	• Loss or degradation of LMR communications • Ineffectiveness or redirection of response operations
Overloaded communications network as a result of an unintentional threat results in denial of service conditions for public safety and emergency services communications networks	• Inability of the general public to access emergency services • Inability to effectively deploy resources
Emergency Medical Services	
Risk	*Operational Impacts*
Lack of availability of sector database as a result of an unintentional threat causes disruption of mission capability	• PSAP system failure (misdirected or no dispatches) • Inability to access subject matter affecting emergency response procedures
Compromised sector database as a result of an unintentional threat causes corruption of critical information	• Slowed overall response time • Inability of internal staff to trust integrity of data, putting all entries in doubt
Public alerting and warning system disseminates inaccurate information as a result of an unintentional threat	• Redirection of first responders to false alarms/ wasting resources • Public confusion and panic

Emergency Management	
Risk	*Operational Impacts*
Public alerting and warning system disseminates inaccurate information as a result of an unintentional or deliberate threat	• Redirection of first responders to false alarms/wasting of resources • Action by the public that is inaccurate/ unwarranted, creating distrust and reducing effectiveness of operations
Loss of communications lines as a result of a deliberate threat results in disrupted communications capabilities	• Loss or degradation of 9-1-1 services • Ineffectiveness or redirection of response operations
Overloaded communications network as a result of an unintentional threat results in denial of service conditions for public safety and emergency services communications networks	• Inability of the general public to access emergency services • Loss of confidence in emergency services
Public Works	
Risk	*Operational Impacts*
Compromised sector database as a result of an unintentional threat causes corruption of critical information	• Loss of service, including electrical, water, wastewater • Overall response time slowed
Loss of communications lines as a result of an unintentional or deliberate threat results in disrupted communications capabilities	• Loss or degradation of 9-1-1 services • Ineffectiveness or redirection of response operations
CCTV jamming/blocking as a result of a deliberate threat causes disrupted surveillance capabilities	• Inability to monitor/respond to physical incident • Failure to record evidence/criminal acts

Public Safety Communications and Coordination/Fusion	
Risk	*Operational Impacts*
Natural disaster causes loss of 9-1-1 capabilities	• Unavailability of certain critical systems; possible inability to coordinate incident response or stay notified of incidents • Reduced effectiveness of element coordination
Lack of availability of sector database as a result of an unintentional or deliberate threat causes disruption of mission capability	• PSAP system failure • Redirection of resources leading to slow response and unavailability of some systems
Loss of communications lines as a result of an unintentional threat results in disrupted communications capabilities	• Loss or degradation of 9-1-1 services • Ineffectiveness or redirection of response operations

5.2. Next Steps

Although access to new cyber technology has enabled ESS to expand and improve its operational ability across disciplines, there has been growing concern regarding attacks on critical infrastructure. Threats against cyber infrastructure have grown rapidly in the past few years as hackers, hacktivists, cyber criminals, terrorists, and sophisticated State and non-State actors have exploited vulnerabilities motivated by a variety of objectives.

The results of the ESS-CRA show that cyber threats can have a significant impact on the ESS disciplines' ability to operate. It is important for ESS stakeholders, such as cyber infrastructure owners, acquirers, managers, policy makers, and operators, to stay aware of current and upcoming cyber threats and focus on implementing security before, rather than after, an incident occurs. Although this assessment addresses several strategic risks to the ESS infrastructure that are of national concern based upon the knowledge and subject matter expertise of those participating in ESS's risk assessment activities, this assessment does not address all risk scenarios faced by ESS entities or their users and customers. Other cyber threat areas require additional collaborative study and further review by ESS stakeholders.

The next step in CARMA after the ESS-CRA is to determine how risks should be addressed. This will enable ESS to determine which of the four risk management options—accepting, avoiding, transferring, or mitigating a cyber risk—is the most appropriate response to the risks identified in the ESS-CRA. To consider these four options in a comparable way, CARMA provides a process through which ESS stakeholders can discuss and evaluate various factors that help determine the appropriate cyber risk response. ESS will develop and release the *Emergency Services Sector Cybersecurity Roadmap* to outline the risk responses for each of the risks identified through CARMA and captured in the ESS-CRA. This roadmap will describe the ESS cybersecurity risk management strategy.

Appendix A: Emergency Services Sector Cyber Infrastructure and Use in Value Chains

Law Enforcement		
Cyber Technology/ Resource	**Description**	**Cyber Technology/Resource Application**
Computer Aided Dispatch	CAD systems refer to the variety of computer resources used to aid emergency dispatchers.[18] CAD systems give dispatchers and call takers the ability to receive telephone calls from the public, quickly determine the origin and nature of 9-1-1 calls, and transmit processed requests in a fraction of the time that would be required if this task were performed manually. On demand, dispatchers query the system about processed requests that are pending action and seek recommendations from the system for the most appropriate response for each request. If the dispatcher agrees, the request is quickly transmitted via wireless connection to available field forces.	❑ GATHER, COLLECT CAD systems are used to gather information from callers and field forces, and to collect the data in a useable form. ❑ ANALYZE CAD systems analyze data and develop response recommendations. The dispatcher can seek a recommendation, agree, and transmit the recommendation. Alternatively, the dispatcher can disagree and dispatch resources based on his/her own recommendations. ❑ SHARE, COMMUNICATE, NOTIFY CAD systems permit end users to share data among those allowed to query information. They support data communications such as text messaging between end users and dispatchers. They permit dispatchers to send assistance requests when more resources are needed. ❑ SERVE, RESPOND, OPERATE End users use CAD terminals to acknowledge the dispatch of resources, indicate responses, and notify others of arrival using status changes in the system, which automatically records associated times and event numbers for each request. End users can then use the CAD terminal in the communications center or in their vehicles while operating on the scene of an incident to query various databases and research history for a particular address or incident. ❑ RECORD, SAVE, REVIEW End users add text to enhance the geospatial and public safety knowledge about the premises involved in incidents. The end results are retained for criminal justice purposes, and inform planning and research activities to improve resource deployment, reduce response times, and justify increasing or decreasing resource allocations. Some CAD systems also offer Records

[18] CAD computer resources include criminal justice databases, motor vehicle administration databases, geographical information systems , police resource deployment plans, the automatic number indicator and automatic location indicator records provided by plain old telephone system providers, and callers seeking law enforcement assistance

		Management Systems (RMS) capable of supporting not just CAD records, but incident reporting software, including national incident reporting system-compliant software, that permits either over-the-air submission or external drive and hard disk downloads to desktop terminals at stations.
Criminal Justice Networks and Systems	Law enforcement officers use a variety of Federal, State, and local criminal justice networks. These networks, and the services they provide, are accessed via private wired and wireless terminals and connections. For example, the National Law Enforcement Telecommunications System (NLETS) links local, State, and many Federal law enforcement agencies for the purposes of communicating criminal justice information and sharing access to criminal justice databases. In addition, the NCIC collects and shares criminal justice information about wanted and missing persons, as well as lost and stolen property. NCIC is a database resource created, maintained, and operated by the FBI. The FBI requires that all law enforcement personnel that access NCIC complete a rigorous training and certification program regularly, that terminals and their locations have restricted access, and that terminals be used solely for criminal justice purposes. Users are expressly prohibited from connection with the Internet or other non-law enforcement networks or communications systems. Other popular criminal justice services that use cyber resources include fingerprint and photo identification databases, and networks that link to jail management systems.	❑ GATHER, COLLECT These systems provide a repository for victim and witness information, contacts by law enforcement officers with the public, criminal history, the existence and status of warrants for arrest, the names and descriptions of persons missing or wanted, and the makes, models, serial numbers, and descriptions of lost and stolen articles. ❑ ANALYZE These systems provide analysis, using data from databases to find commonalities that may have investigative value, such as crime site patterns or names that recur from contacts at crime scenes. Fingerprint and identification databases provide rapid analysis of electronic print cards to search for suspects with prior criminal justice contacts. ❑ SHARE, COMMUNICATE, NOTIFY These systems provide agencies with the ability to send inquiries to other law enforcement agencies in their region, their State, or nationwide to seek information about crimes that may indicate a larger pattern of incidence, or perpetrator(s) operating in more than one jurisdiction Agencies can share data, notify surrounding agencies to be on the lookout for wanted persons or vehicles involved in crimes, and notify other agencies of the occurrence of major crimes or disasters that may require force multiplication to conduct searches or manhunts, or urgent response. Interfaces with jail management networks permit investigators to determine whether suspects they want are already incarcerated. ❑ SERVE, RESPOND, OPERATE These systems are used by law enforcement officers to query a database, either independently or with the assistance of dispatchers. They may do this while on patrol, when they encounter suspicious people or vehicles, or while on the scene of a crime to support their investigation. ❑ RECORD, SAVE, REVIEW These systems are used by law enforcement agencies to enter, modify, and withdraw data from various databases using criminal justice systems and networks. NCIC, for example, requires that the State police agency in every State audits the local, State, and tribal law enforcement agencies to assure that only staff members who are trained, certified, and authorized are accessing the system,

		that record keeping is organized and up-to-date, and that all entries meet FBI criteria. Fingerprint and photo identification databases provide electronic entry and storage in vast systems for rapid retrieval when the data is needed or a new search for data is desired.
Geospatial Tools and Systems	Geospatial tools and systems include such resources as GIS databases, which contain critical infrastructure features such as utility placement, government facility types and locations, and property plats. They also include mapping data, services such as Automated Vehicle Location (AVL) to support more effective use of CAD systems, latitude and longitude conversion from GIS-enabled mobile telephony to learn nearest street addresses, and situational awareness applications that permit end users, dispatchers, and supervisors to see the deployments of resources for specific incidents or events. These tools and systems may be used to provide field forces with navigational aids or provide dispatchers with a display of geospatial information to understand routes of travel and escape. They provide data to inform intelligence link analysis tools as well. Computer-aided drawing packages help victims and witnesses to identify criminal perpetrators through software packages that can create sketches in the absence of photographs.	❑ GATHER, COLLECT Systems and tools are used by law enforcement agencies to gather and collect characteristics of a crime, such as victims, witnesses, suspects, lookouts, weapons used, articles taken, locations, dates, times, and weather. ❑ ANALYZE Systems and tools are used by law enforcement personnel, typically crime analysts or investigators, to predict when and where future crimes may occur to develop strategies that can be used to solve cases and convict criminal offenders. ❑ SHARE, COMMUNICATE, NOTIFY Systems and tools are used by law enforcement agencies to share data within their organization or with other jurisdictions and agencies to create force multiplication in their efforts to predict, detect, and locate crimes, as well as arrest criminal offenders. Such communications may also be used to populate intelligence linking systems to detect other commonalities. ❑ SERVE, RESPOND, OPERATE Law enforcement agencies use the products that geospatial tools and systems yield to effect resource deployments, conduct patrol patterns and practices, respond more effectively, and operate more safely based on increased situational awareness. ❑ RECORD, SAVE, REVIEW Systems and tools are used to locate articles or materials of evidentiary value and provide a geographic history to inform crime trends and help plan crime prevention and detection measures. Systems such as AVL are used in real time to inform CAD system response recommendations or to help dispatchers gain situational awareness about deployed resources to manage gaps in coverage, locate personnel or vehicles that are otherwise out of communication, or allow break times for field forces.
Internet	The Internet provides law enforcement agencies with open-source information for research that can be used to detect and locate suspects, track criminal information offers, conduct outreach, and inform the public. Tools such as social networking sites (Twitter®, Facebook®, MySpace®,	❑ GATHER, COLLECT Law enforcement agencies use the Internet to conduct open-source research that may help them identify suspects, locate missing or wanted persons, collect crime-solving tips, or even learn about crimes that have not yet been officially

	and others) provide a means of readily communicating crime prevention tips, witness and suspect information, and provide official news and directions for end users in the event of an emergency.	reported. ❑ ANALYZE The Internet provides a variety of information about crimes and suspects, from incidents yet to be officially reported or investigated, to suspects posting stories or bragging about their exploits online. Computer forensic specialists can then analyze content and work with Internet service providers to locate the originating computers to find missing or wanted persons. ❑ SHARE, COMMUNICATE, NOTIFY The Internet provides agencies with the ability to interact with the public via electronic mail, social media sites, or Web pages to prevent, detect, and solve crimes. Many agencies encourage electronic reporting of instances of abuse of authority or excessive force by their officers, and to provide a means of reaching senior officials to offer compliments or complaints. Nearly all law enforcement agencies use the Internet to transmit and receive electronic mail for internal purposes. ❑ SERVE, RESPOND, OPERATE The Internet provides computing resources that permit officers to send text messages or electronic mail while deployed in the field or in quarters, depending on agency policies. ❑ RECORD, SAVE, REVIEW The Internet allows the public to submit correspondence via the Internet that can be saved for an official response. Text messages may not be saved for historical purposes but may be reviewed to assure proper use of time and resources.
Radio Infrastructure	Law enforcement agencies use spectrum in the aviation, land mobile, and marine radio bands to conduct patrol, response, search, and rescue operations. In the LMR band alone, they operate in both the very high frequency (VHF)/high band and VHF/low band, and in the ultra high frequency (UHF)/460 megahertz (MHz), UHF-T/470 MHz, and UHF/800 MHz bands. Although there are still a considerable number of analog and conventional radio systems in use, more and more agencies are adopting other configurations (such as digital systems or trunked systems) as a result of modernization or mandates (for example, the Federal Communications Commission (FCC) requires that all local and State public safety agencies move from wideband to narrowband configurations no later than December 31, 2013). As system operators migrate to modern infrastructure,	❑ GATHER, COLLECT In emergencies, radio infrastructure is used by law enforcement officers to report crimes or incidents that they come upon during patrol. Both dispatchers and officers may use radios to gather descriptions broadcast via lookouts. ❑ ANALYZE Modern radio infrastructure may offer information systems that analyze capacity and call load for internal purposes. ❑ SHARE, COMMUNICATE, NOTIFY Radio infrastructure is used by dispatchers and law enforcement officers to share, communicate, and notify. While voice communications make up the vast majority of traffic, some radio systems permit field forces to send urgent traffic via activation of an emergency switch located on the end user's radio to alert dispatchers when that user is at high risk and needs immediate assistance.

	many are also switching to systems that use IP technology to propagate signals.	❑ SERVE, RESPOND, OPERATE Radio infrastructure is used to receive assignments, broadcast status changes, request resources, check on wanted persons, and provide situational awareness to peers and supervisors. This cyber resource is critical to officer safety, providing an immediate means of reporting trouble and requesting assistance. ❑ RECORD, SAVE, REVIEW Radio infrastructure is s used to record all radio traffic in a given period. Recordings are saved for investigative and informational purposes and to support training and procedural improvements.
Security and Surveillance Systems	Law enforcement agencies with patrol and incident response roles are routinely called to investigate the activation of security alarm systems at businesses and residences. Such systems may be passive (arranged to detect intrusion through windows and doors via a wide array of technology) or active (designed to be manually activated, such as the switches that bank tellers and cashiers use when they are being robbed). The systems may trigger silent alarms (those that make no sound or light a visual aid to prevent criminals from learning their presence has been detected, which may prevent hostage-taking or punishment for activating the system) or audible alarms (which may or may not include visual signals such as warning lamps to encourage criminals to leave immediately), depending on the premises protected. Some security systems also include supervisory features to detect tampering with system components or connectivity lines. Some systems may be local systems that do not transmit activations to monitoring (central stations) services. Law enforcement agencies themselves may rely on security systems to protect isolated or sensitive locations, such as property yards, evidence rooms, armories, or radio tower sites. Law enforcement agencies may also operate surveillance systems that permit them to use cameras and closed circuits to observe activities in high-crime areas, high-security areas, college campuses, or their own facilities, including detention cells, hallways, sally ports, and parking lots.	❑ GATHER, COLLECT Systems may have the ability to record audio and/or video at protected premises. ❑ ANALYZE Systems may provide data that can be analyzed at a later time. ❑ SHARE, COMMUNICATE, NOTIFY Systems may offer connectivity to transmit activations to monitoring stations for review and action. Some systems include annunciation information that permits field forces to know the type of alarm activated (manual or automatic, burglary, holdup, or panic) and location (such as front door, basement window on the south side). ❑ SERVE, RESPOND, OPERATE Monitoring live surveillance systems through a closed circuit can help dispatchers to direct field forces to broken windows, points of entry, and even the direction that fleeing suspects may be leaving. They can also help dispatchers understand whether injuries have been incurred to prompt them to send EMS with law enforcement. ❑ RECORD, SAVE, REVIEW Many surveillance systems include either hard or soft recording media that can be retrieved for analysis and that can become part of the case record for a given crime. Products such as video recordings can be instrumental in criminal prosecution and determination of guilt.
Tele-communications Services	Law enforcement agencies use a variety of telecommunications services, from POTS to pagers, PDA to smartphones, cellular telephones, and ESMR to conduct and support interaction with the general public,	❑ GATHER, COLLECT Call takers use POTS and IP-based or GUI-enhanced telephone systems to receive and process calls for dispatch and to make notifications to allied services such as fire and rescue, towing

	crime victims, and witnesses; coordinate investigative leads; and conduct administrative business. Although many agencies are still using original 1A2 keyset technology in their telephony, the use of IP-based and graphical user interfaces (GUI) has begun to modernize the citizen-to-authority and authority-to-citizen (such as Reverse 9-1-1®) communications. Under the provisions of the Americans with Disabilities Act, law enforcement communications centers are required to provide equal access to emergency telephone numbers and so they use teletype (TTY) or other telecommunications devices for the deaf (TDD) to intercommunicate with the deaf and hard of hearing populations they serve. Data exchange hubs may be used to link telecommunications systems to support automatic and mutual aid, broad criminal investigations, or for administrative messaging and other interagency communications over data or video systems. Other systems may include Variable Message Boards (VMB) to communicate warnings, such as advising motorists about checkpoints ahead, or to issue Amber or Silver Alerts.	companies, public utilities, etc. ❑ ANALYZE Call takers use these services for supporting software and connectivity with other agencies. A notable exception is Enhanced and Next Generation 9-1-1 services, which permit call takers in communications centers to receive automatic number identification (ANI)/automatic location identification (ALI) and analyze the data to verify the telephone numbers and addresses for callers. This simple analysis helps assure that law enforcement field forces are sent to the correct location every time. ❑ SHARE, NOTIFY, COMMUNICATE Telephony is used to place and receive calls, make notifications, conduct administrative business, and communicate with the public. Some agencies are interconnected with data exchange hubs to permit communications among criminal justice networks, administrative messaging systems, CAD systems, or other telecommunications resources used by other agencies in the same functional area, in different functional areas, or across levels of government. ❑ SERVE, RESPOND, OPERATE Services are used to facilitate response of allied services (tow trucks, power companies, medical examiners, etc.) to serve the public. Devices such as VMB may be used to support special or long-term operations and disaster response and recovery. ❑ RECORD, SAVE, REVIEW Systems such as PDA devices and smart phones offer voice, data, and video capabilities that can capture and record images and information in a manner that can be retrieved or saved onto more permanent electronic data storage systems for future review. Enhanced and Next Generation 9-1-1 systems record the details of every call a communications center receives, such as date/time, ANI/ALI, times to answer, and duration of the call, which can be helpful to investigating complaints, substantiating reports of lost connectivity with telephone company switching offices, and criminal acts. TTY and TDD systems use text messaging to communicate, which offers the option of printing records of conversations in much the same way that logging recorders collect voice traffic.
Watch and Warning Systems	Law enforcement agencies most commonly use systems such as Reverse 9-1-1 for alerting the public, although social media is being more widely adopted in the community. Legislation passed in the last	❑ SHARE, NOTIFY, COMMUNICATE Software that is dependent on other cyber communications resources is used to facilitate dissemination of alerting messages. In many cases, neither Amber nor Silver Alerts to notify the

	few years has created new cyber venues for public alerting by law enforcement (e.g., Amber Alerts and Silver Alerts).	public to locate missing and endangered juveniles and elderly adults are software packages; they simply use TTY and VMB systems to convey messages. ❑ SERVE, REPORT, OPERATE Devices such as VMB may be used to support special or long-term operations and disaster response and recovery. ❑ RECORD, SAVE, REVIEW Systems are used to support law enforcement efforts but these systems generally do not record or save the data disseminated for later review.

Fire and Emergency Services		
Cyber Technology/ Resource	**Description**	**Cyber Technology/Resource Application**
Computer Aided Dispatch	CAD systems serve the fire and emergency services by combining the electronic resources from GIS, fire and rescue resource deployment plans, ANI and ALI records provided by POTS providers; and callers reporting fires, medical emergencies, HAZMAT releases, and other emergencies that require their assistance. CAD systems give dispatchers and call takers the ability to receive telephone calls from the public, quickly determine the origin of the call, ascertain the nature of the need for fire and emergency services assistance, and transmit processed requests in a fraction of the time required if this task was performed manually. On demand, dispatchers can query the system about processed requests that are pending action and seek a recommendation from the system on the most appropriate response for each request. If the dispatcher agrees, the request is quickly transmitted via wireless connection to field forces available.	❑ GATHER, COLLECT CAD systems are used to gather information from callers and field forces, and to collect the data in a useable form ❑ ANALYZE CAD systems analyze data and develop response recommendations. The dispatcher can seek a recommendation, agree, and transmit the recommendation. Alternatively, the dispatcher can disagree and dispatch resources based on his/her own recommendations. ❑ SHARE, COMMUNICATE, NOTIFY CAD systems permit end users to share the data among end users who have access to query the information. They support data communications such as text messaging between end users and dispatchers. They permit dispatchers to send assistance when more resources are needed. ❑ SERVE, RESPOND, OPERATE End users use CAD terminals to acknowledge the dispatch of resources, indicate responses, and notify others of their arrival using status changes in the system, which automatically records associated times and event numbers for each request. End users can then use the CAD terminal in the communications center or in their vehicles during the course of operating on the scene of an incident to query various databases and research history for a particular address or incident. Fire terminals in responding apparatus can also access geospatial information such as

		the location of fire hydrants and the size of the water mains that supply them, or the approved plans for a building's layout. They can also access files that provide drawings of building features and lots, and determine whether the addresses to which they are responding are known to store HAZMAT and in what forms and quantities. ❑ RECORD, SAVE, REVIEW End users add text to enhance the geospatial and public safety knowledge about the premises involved in incidents. The end results are retained firefighter safety purposes, and inform planning and research activities to improve resource deployment, reduce response times, and justify increasing or decreasing resource allocations. Some CAD systems also offer RMSs capable of supporting not just CAD records, but incident reporting software, including national incident reporting system-compliant software, that permits either over-the-air submission or external drive and hard disk downloads to desktop terminals at stations.
Fire and Medical Alarm Systems	Firefighting and emergency service agencies routinely respond to investigate the activation of fire and medical alarm systems at businesses and residences. Such systems may be passive (set up to detect smoke, a rapid rise of heat, or the movement of water in a sprinkler system via a wide array of technology) or active (designed to be manually activated, such as the call buttons found in senior living facilities, or manual pull stations located throughout commercial buildings and high-rise structures). These systems may trigger silent alarms (those that make no sound or light a visual aid but send a signal to a central station to alert monitoring operators to dispatch medical aid) or audible alarms (which may include pre-recorded voice commands and include visual signals such as warning lamps or strobes to encourage occupants to leave a building immediately) depending on the premises protected. Some systems also include supervisory features to detect tampering with system components or connectivity lines. Some systems may be local systems that do not transmit activations to monitoring (central stations) services. Fire and emergency service agencies themselves may rely on fire alarm systems to protect fire stations and sleeping quarters.	❑ GATHER, COLLECT Systems may provide the ability to record audible warnings to provide voice commands to occupants at protected premises. ❑ ANALYZE Systems may provide data that can be analyzed at a later time. ❑ SHARE, COMMUNICATE, NOTIFY Systems may offer connectivity to transmit activations to monitoring stations for review and action. Some systems may also provide enunciator panels' onsite that permit responding units to determine the type of alarm activated (manual or automatic, medical, smoke, heat, or water flow) and location (such as Apartment 302, the basement area, in a duct, etc.). ❑ SERVE, RESPOND, OPERATE Central station operators can provide fire dispatchers with details about the protected premises. For example, if systems activated include smoke, heat, and water flow detections at an industrial facility, responding firefighters can deduce that an actual fire may be burning and make a determination about the sort of hose lines they should deploy. ❑ RECORD, SAVE, REVIEW Many fire and medical alarm systems are configured to transmit activation signals to a central station. Those signals are recorded, manually or automatically, for later retrieval to

		assist in reviewing response time or to investigate intentional fires. These records can become a part of the case record for a given arson crime.
Geospatial Tools and Systems	Geospatial tools and systems include such resources as GIS databases, which contain critical infrastructure features such as utility placement, government facility types and locations, and property plats. They also include mapping data, services such as AVL to support more effective use of CAD systems, and situational awareness applications that permit end users, dispatchers, and supervisors to see the deployments of resources for specific incidents or events. These tools and systems may be used to provide field forces with navigational aids, or provide dispatchers with a display of geospatial information to understand routes of travel and escape. They provide data to inform intelligence link analysis tools as well. Computer-aided drawing packages help firefighters develop detailed driving instructions that take them from their fire stations to every address for which they are primarily responsible, displaying the locations of fire hydrants, sprinkler connections, fire control rooms, or other features of interest.	❑ GATHER, COLLECT Systems and tools permit fire and emergency service agencies to gather and collect characteristics of a particular business or target hazard, such as topology, proximity to public utility easements and transportation routes, and the layout of industrial campuses and parks. ❑ ANALYZE Firefighters, HAZMAT response teams, inspectors, and others use GIS and geospatial tools to analyze the results of prior responses, to predict the water flow requirements to address major incidents (fires or HAZMAT releases), or to predict when and where arsons may occur based on fire-setting trends. These systems help command staff develop effective firefighting and HAZMAT confinement and containment strategies for target hazard locations. ❑ SHARE, COMMUNICATE, NOTIFY Once strategies are developed, fire and emergency services agencies can use geospatial systems and tools to share that data within their organization or with other jurisdictions and agencies to create force multiplication in their efforts to effectively, efficiently, and safely respond to emergencies. ❑ SERVE, RESPOND, OPERATE Fire and emergency service agencies use the products that geospatial tools and systems yield to effect resource deployments, conduct tactical firefighting practices, respond more effectively, and operate more safely based on increased situational awareness. ❑ RECORD, SAVE, REVIEW Systems such as AVL are used in real-time to inform CAD system response recommendations or to help dispatchers gain situational awareness about deployed resources to manage gaps in coverage or locate response resources that are otherwise out of communication.
Internet	The Internet provides fire and emergency service agencies with open sources for research that can be used to gain insights about emergencies occurring elsewhere to glean lessons learned, identify source materials for training, code enforcement, or to learn about the properties, risks, and tactical	❑ GATHER, COLLECT Fire and emergency service agencies use the Internet to conduct open-source research that may help them learn about how major incidents in their region, in their State, or even around the world, are being addressed. They may also use

	responses most appropriate for the confining and containing fires and spills from hazardous materials databases. They may also use the Internet to conduct outreach and deliver life safety education to the public. Tools such as social networking sites (Twitter®, Facebook®, MySpace®, and others) provide a means of readily communicating fire prevention tips, updates on significant incidents. Many fire and emergency service agencies use the Internet to provide official news and directions for the public in the event of an emergency.	HAZMAT databases to learn about the characteristics of a material they encounter, such as its chemical properties, how water may affect a fire or spill, and the most appropriate distances surrounding a spill or fire from which evacuations should be conducted. ❑ ANALYZE Social networking sites provide a variety of information about fires and other emergencies based on interaction between the agency and the public. Arson suspects posting stories or bragging about their exploits online may be detected and located. Data on specific HAZMAT can be analyzed to develop a strategy and tactical plan to address evacuations, confinement, and containment efforts. ❑ SHARE, COMMUNICATE, NOTIFY The Internet provides agencies with the ability to interact with the public via electronic mail, social media sites, or W-eb pages to prevent, detect, and solve crimes. Many agencies encourage electronic communications to offer compliments or complaints. Nearly all fire and emergency service agencies use the Internet to transmit and receive electronic mail for internal purposes. ❑ SERVE, RESPOND, OPERATE Many HAZMAT response teams possess computing resources that permit their leaders to send text messages or electronic mail while deployed in the field. These capabilities may be used to interact with chemists or other specialists who can provide insights on the properties and behaviors of specific materials that have been released. Few fire service agencies have this same level of Internet access. Thus, Internet access is most often accomplished when in quarters. ❑ RECORD, SAVE, REVIEW Some agencies permit the public to submit correspondence via the Internet that can be saved for an official response. Text messages may not be saved for historical purposes but may be reviewed to assure proper use of time and resources.
Modeling and Simulation Tools	Fire and emergency services agencies use a variety of modeling and simulation tools to aid in operations such as wildfire suppression and HAZMAT emergencies. They are used to predict the movement of smoke and fire and the spread of toxic or otherwise polluting bases and liquids as a result of a spill or other release.	❑ GATHER, COLLECT Fire and emergency service agencies use sources such as weather observations and predictions, the amount of moisture in ground fuels, topographical mapping data, the fuels involved in a wildfire, and the numbers of firefighters and firefighting apparatus and equipment committed to the scene and in reserve. They may gather similar inputs, along

		with chemical properties and environmental features (such as proximity to streams, lakes, ponds, or underground water supplies, or to highways and target hazards) to develop models and simulations for HAZMAT materials releases. ❑ ANALYZE Once modeling and simulation tools have been populated with the necessary data, fire and emergency service agencies use them to develop models that help incident commanders understand whether tactical adjustments in their strategic plans must be made, whether the strategy needs to be modified, or whether additional resources should be called up or dismissed. They may also use similar inputs to learn how water (from rainfall, snowfall, or firefighting operations) may affect a fire or spill, and the most appropriate distances surrounding a spill or fire from which evacuations should be conducted. ❑ SHARE, COMMUNICATE, NOTIFY Many simulation tools permit sharing with other agencies via wired or wireless communications devices. ❑ SERVE, RESPOND, OPERATE Many hazardous materials response teams possess computing resources that permit activities such as plume modeling, environmental impacts, and evacuation planning, which inform the incident priorities that must be accomplished. Wildfire modeling and simulation tools can have a dramatic impact on the assignment and deployment of available resources, and the establishment of staging operations in order to have necessary resources on hand when models predict a change in offensive or defensive, direct or indirect, firefighting operations. ❑ RECORD, SAVE, REVIEW The most prevalent modeling and simulation tools develop products that can be saved and reviewed at any time to glean lessons learned or to document activities performed.
Personal Alert Safety Systems (PASS)	Fire and emergency services personnel frequently operate in environments characterized by an imminent danger to life and health (IDLH). This requires them to don specialized personal protective ensembles that may be partly or fully encapsulated, that inhibit movement, and that have angles and equipment edges that can be easily snagged or entangled when operating in poor visibility. Because of the inherent dangers in IDLH work	❑ GATHER, COLLECT Most PASS devices neither gather nor collect any data. However, as biological monitoring PASS devices evolve, it is likely that they will all collect data on a regular cycle. ❑ ANALYZE Most PASS devices are incapable of analysis beyond sensing that a wearer has been motionless for 30 seconds or longer. Biological

	and the complications posed by having to wear protective ensembles, PASS systems were created. PASS devices may be manually activated (by a switch that the device wearer pushes) or passively activated (by the device detecting that the wearer has been motionless for 30 seconds or longer). The activation results in emission of a shrill sound to alert others in listening distance that a colleague is in trouble or may be down and needs immediate rescue. PASS devices are frequently attached to or integrated with the Self Contained Breathing Apparatus (SCBA) that a firefighter or HAZMAT technician may be using. PASS products have evolved from local alarms to alert others operating in close proximity that a firefighter or HAZMAT technician may be in trouble, to systems supported by RF technology that permits the activation of such systems to be transmitted to incident commanders, who use special receivers that identify the wearer, permitting quick assignment of fellow crew members to locate and assist the wearer of the activated device. These devices that use RF technology are exposed to cyber risks and threats, just as any radio-operated communications system would be. PASS devices are also evolving to include passive biological monitoring equipment that, rather than being worn on the SCBA, may be integrated into the ensemble or worn as a vest with built-in sensing technology. These biological PASS devices can detect the wearer's body temperature, pulse, blood pressure, and respirations, as envisioned, although the technology to accomplish these monitoring tasks is still emerging. A sudden spike in any of the monitored vital signs can cause transmission of an alarm to the incident commander, who can then act to have the affected wearer relieved and brought out for medical evaluation, or if necessary, transportation to a hospital. Biological monitoring PASS devices use RF technology and thus may also have their transmissions jammed, blocked, spoofed, or altered.	monitoring PASS devices detect variations from normal findings and transmit alarms to bring such findings to the attention of an incident commander. ❑ SHARE, COMMUNICATE, NOTIFY Most PASS devices share activations through piercing audible alarms to alert others in proximity of the wearer. Some PASS devices can use RF technology to alert incident commanders to activations. Some biological monitoring PASS devices can also transmit findings of significant vital sign abnormalities to the incident commander. ❑ SERVE, RESPOND, OPERATE Firefighters and HAZMAT technicians use PASS devices every time they don their personal protective ensembles. An inherent problem in older PASS devices is that they require the user to manually activate the device to begin monitoring movement and/or to sound an alarm when the wearer is in trouble. Systems that are integrated with SCBA are usually designed to activate when the airflow in the apparatus is started. ❑ RECORD, SAVE, REVIEW PASS devices that incorporate RF technology vary in their ability to record and save data, but most popular brands are capable of doing so. Biological monitoring PASS devices also transmit data that is recorded and saved. In both instances, the data can provide invaluable assistance in populating medical records, providing safety lessons, or aiding in investigations of illnesses, injuries, or deaths of the wearers.
Radio Infrastructure	Fire and emergency service agencies use spectrum in the aviation, land mobile, and marine radio bands to conduct patrol, emergency response, search, and rescue operations. In the LMR band alone, they operate in both the VHF/high band and VHF/low band, and in the UHF/460 MHz, UHF-T/470 MHz, and UHF/800 MHz bands. Although there are still a considerable number of analog and conventional radio systems in use, more and more agencies are adopting other configurations (such as digital systems	❑ GATHER, COLLECT Radio systems may be used in emergencies by firefighters or other emergency service responders to report crimes or incidents that they come upon during local travel. Both dispatchers and fire officers may use radios to gather descriptions or to request additional resources. ❑ ANALYZE Modern radio infrastructure may offer

	or trunked systems) as a result of modernization or mandates (for example, the FCC requires that all local and State public safety agencies move from wideband to narrowband configurations no later than December 31, 2013). As system operators migrate to modern infrastructure, many are also switching to systems that use IP technology to propagate signal.	information systems that analyze capacity and call load for internal purposes, but such capabilities are not end user features. ❑ SHARE, COMMUNICATE, NOTIFY Radio infrastructure is routinely used by dispatchers and firefighting and emergency services providers to share, communicate, and notify. While voice communications make up the vast majority of traffic, some radio systems permit field forces to send urgent traffic via activation of an emergency switch located on the end user's radio to alert dispatchers when that user is at high risk and needs immediate assistance. ❑ SERVE, RESPOND, OPERATE Radio infrastructure is a critical component in delivering fire and emergency service. Personnel use radios to receive assignments, broadcast status changes, request resources, coordinate with mutual aid agencies, and provide situational awareness to their peers and supervisors. This cyber resource is critical to firefighter safety, providing an immediate means of reporting trouble and requesting assistance when they might otherwise be separated from other members of their crew. ❑ RECORD, SAVE, REVIEW Most fire and emergency service agencies use logging recorders to record all radio traffic in a given period, and they save these recordings for investigative and informational purposes and to support training and procedural improvements.
Tele-communications Services	Fire and emergency service agencies use a variety of telecommunications services, from POTS to pagers, PDAs to smartphones, cellular telephones, and ESMR to conduct and support interaction with the general public, coordinate investigative leads, and conduct administrative business. Although many agencies are still using original 1A2 keyset technology in their telephony, the use of IP-based and user-friendly GUIs has begun to modernize the citizen-to-authority and authority-to-citizen (such as Reverse 9-1-1®) communications. Under the provisions of the Americans with Disabilities Act, fire and emergency service communications centers are required to provide equal access to emergency telephone numbers and so they use TTY or other TDD to intercommunicate with the deaf and hard of hearing populations they serve.	❑ GATHER, COLLECT Call takers use POTS and IP-based or GUI-enhanced telephone systems to receive and process calls for dispatch and to make notifications to allied services such as law enforcement, public utilities, etc. ❑ ANALYZE Telecommunications services generally are not used to analyze information, but the networks over which these services operate are often used for supporting software and connectivity with other agencies. A notable exception is Enhanced and Next Generation 9-1-1 services, which permit call takers in communications centers to receive ANI/ALI and analyze the data to verify the telephone numbers and addresses for callers. This simple analysis helps assure that fire and emergency service personnel are sent to the correct location every time. ❑ SHARE, NOTIFY, COMMUNICATE Fire and emergency service agencies use

		telephony to place and receive calls, make notifications, conduct administrative business, and communicate with the public. ❑ SERVE, RESPOND, OPERATE Telecommunications services are routinely used to serve the public to facilitate response of allied services (tow trucks, power companies, gas companies, etc.). ❑ RECORD, SAVE, REVIEW Telecommunications systems such as PDA devices and smartphones offer voice, data, and video capabilities that can capture and record images and information in a manner that can be retrieved or saved onto more permanent electronic data storage systems for future review. Enhanced and Next Generation 9-1-1 systems record the details of every call a communications center receives, such as date/time, ANI/ALI, times to answer, and duration of the call which can be helpful to investigating complaints, substantiating reports of lost connectivity with telephone company switching offices, and criminal acts. TTY and TDD systems use text messaging to communicate, which offers the option of printing records of conversations in much the same way that logging recorders collect voice traffic.

Emergency Medical Services		
Cyber Technology/ Resource	**Description**	**Cyber Technology/Resource Application**
Computer Aided Dispatch	CAD systems serve EMS agencies by combining the electronic resources from GIS, resource deployment plans, ANI and ALI records provided by POTS providers; and callers reporting illnesses, injuries, or other emergencies that require their assistance. CAD systems give dispatchers and call takers the ability to receive telephone calls from the public, quickly determine the origin of the call, ascertain the nature of the need for fire and emergency services assistance, and transmit processed requests in a fraction of the time required if this task was performed manually. On demand, dispatchers can query the system about processed requests that are pending action and seek a recommendation from the system on the most appropriate response for each request. If the dispatcher agrees, the request is quickly transmitted via wireless connection to field forces available.	❑ GATHER, COLLECT CAD systems are used to gather information from callers and field forces, and to collect the data in a useable form. ❑ ANALYZE CAD systems analyze the data and develop response recommendations. The dispatcher can seek a recommendation, agree, and transmit the recommendation. Alternatively, the dispatcher can disagree and dispatch resources based on his/her own recommendations. ❑ SHARE, COMMUNICATE, NOTIFY CAD systems permit end users to share the data among end users who have access to query the information. They support data communications such as text messaging between end users and dispatchers. They permit dispatchers to send assistance when

		more resources are needed, or to quickly recall resources when they are no longer needed. ❑ SERVE, RESPOND, OPERATE End users use CAD terminals to acknowledge the dispatch of resources, indicate responses, and notify others of their arrival using status changes in the system, which automatically records associated times and event numbers for each request. End users can then use the CAD terminal in the communications center or in their vehicles during the course of operating on the scene of an incident to query various databases and research history for a particular address or incident. EMS terminals in responding units can also access geospatial information such as the approved plans for a building's layout. They can also access files that provide drawings of building features and lots. They may be able to access the response history of an address to determine prior medical complaints that may help inform care providers of what they may encounter. ❑ RECORD, SAVE, REVIEW End users add text to enhance the geospatial and public safety knowledge about the premises involved in incidents. The end results are retained for EMS provider safety purposes, and they inform planning and research activities to improve resource deployment, reduce response times, and justify increasing or decreasing resource allocations. Some CAD systems also offer RMSs capable of supporting not just CAD records, but incident reporting software, including national incident reporting system-compliant software, that permits either over-the-air submission or external drive and hard disk downloads to desktop terminals at stations.
Medical Alarm Systems	EMS agencies routinely respond to investigate the activation of medical alarm systems at assisted living, senior living, or private residences. Such systems are active (designed to be manually activated, such as the call buttons found in senior living facilities or on pendants equipped with RF technology). These systems trigger silent alarms (those that make no sound or light a visual aid but send a signal to a central station to alert monitoring operators to dispatch medical aid) depending on the person or premises protected. Some pendants with RF technology systems may permit voice communications with a central station operator, who can glean the precise medical emergency while notifying the affected EMS agency to respond.	❑ GATHER, COLLECT Medical alarm systems generally have no ability to gather data. Pendants with RF technology can permit central station operators to collect information from persons in need of immediate medical care. ❑ ANALYZE These systems generally do not offer analytical capabilities. ❑ SHARE, COMMUNICATE, NOTIFY Medical alarm systems have connectivity to transmit activations to monitoring stations for review and action. They may also provide annunciator panels onsite that permit responding units to determine the origin of a medical alarm.

		❑ SERVE, RESPOND, OPERATE Central station operators can provide EMS dispatchers with details about the protected person or premises. For example, if system activation originates with a pendant equipped with RF technology, the wearer can inform the central station operator of the emergency at hand, which can be shared with responding EMS personnel. This information can be very helpful in selecting the equipment to take into the building when the responding units arrive. ❑ RECORD, SAVE, REVIEW Many medical alarm systems are configured to transmit activation signals to a central station. Those signals are recorded, manually or automatically, for later retrieval to assist in reviewing response time. These records can become a part of the case record for a given patient's medical history.
Geospatial Tools and Systems	Geospatial tools and systems include such resources as GIS databases, which contain critical infrastructure features such as utility placement, government facility types and locations, and property plats. They also include mapping data, services such as AVL to support more effective use of CAD systems, and situational awareness applications that permit end users, dispatchers, and supervisors to see the deployments of resources for specific incidents or events. These tools and systems may be used to provide field forces with navigational aids, or provide dispatchers with a display of geospatial information to understand routes of travel. Computer-aided drawing packages help EMS agencies develop detailed driving instructions that take them from their assigned quarters to every address for which they are primarily responsible, displaying the locations of elevators, loading docks, annunciator panels, or other features of interest.	❑ GATHER, COLLECT Geospatial systems permit EMS agencies to gather and collect characteristics of a particular business or target hazard, such as topology, proximity to transportation routes and receiving hospital facilities, and the layout of nursing, assisted, and senior living campuses. ❑ ANALYZE EMS agencies use GIS and geospatial tools to analyze the results of prior responses to predict trends in service demands. These systems help the command staff to develop effective plans for resource deployment, negotiate first responder agreements, or determine the need for expansion or relocation of quarters. ❑ SHARE, COMMUNICATE, NOTIFY Once strategies are developed, EMS agencies can use geospatial systems and tools to share that data within their organization or with other jurisdictions and agencies to create force multiplication in their efforts to effectively, efficiently, and safely respond to emergencies. ❑ SERVE, RESPOND, OPERATE EMS agencies use the products that geospatial tools and systems yield to effect resource deployments, determine treatment and transportation protocols based on distance from hospital facilities, evaluate current practices, respond more effectively, and operate more safely based on increased situational awareness. ❑ RECORD, SAVE, REVIEW Systems such as AVL are used in real-time to

		inform CAD system response recommendations or to help dispatchers gain situational awareness about deployed resources to manage gaps in coverage or locate response resources that are otherwise out of communication.
Internet	The Internet provides EMS agencies with open sources for research that can be used to gain insights about emergencies occurring elsewhere to glean lessons learned, identify source materials for training, medical advances, or to learn about the properties and populations they protect. They may also use the Internet to conduct outreach and deliver life safety education to the public. Tools such as social networking sites (Twitter®, Facebook®, MySpace®, and others) provide a means of readily communicating poison and injury prevention tips, and updates on significant incidents. Many EMS agencies use the Internet to provide official news and directions for the public in the event of an emergency. The Internet may also support the electronic transfer of patient care reports using software packages designed to collect and document patient information and medical interventions.	❑ GATHER, COLLECT EMS agencies use the Internet to conduct open source research that may help them learn about how major incidents in their region, in their State, or even around the world, are being addressed. ❑ ANALYZE Social networking sites provide a variety of information about emergencies based on interaction between the agency and the public. ❑ SHARE, COMMUNICATE, NOTIFY The Internet provides agencies with the ability to interact with the public via electronic mail, social media sites, or Web pages to prevent, detect, and solve crimes. Many agencies encourage electronic communications to offer compliments or complaints. Nearly all EMS agencies use the Internet to transmit and receive electronic mail for internal purposes. Electronic Patient Care Reporting (ePCR) systems also provide EMS personnel with a tool to document patient information, medical signs and symptoms, and interventions taken to provide emergency medical care. In turn, these ePCR systems may use the Internet to transfer that data to receiving hospitals, base agencies, billing services, and State health agencies. ❑ SERVE, RESPOND, OPERATE Many EMS agencies possess computing resources that permit their crews to search treatment protocols, consult medical dictionaries and encyclopedias, and send text messages or electronic mail while deployed in the field. These capabilities may be used to reach medical libraries or Web sites that can provide data on the effects of certain medications or toxins, or to identify pills and capsules found outside of labeled containers. ❑ RECORD, SAVE, REVIEW Some agencies permit the public to submit correspondence via the Internet that can be saved for an official response. Text messages may not be saved for historical purposes but may be reviewed to assure proper use of time and resources. The ePCR system that interfaces with the Internet creates a permanent record of patient care provided by EMS user agencies, which can be used for quality

		improvement and training initiatives.
Radio Infrastructure	EMS agencies use spectrum in the aviation and LMR bands to conduct emergency response, search and rescue, and medical evacuation operations. In the LMR radio band alone, they operate in both the VHF/high band and VHF/low band, and in the UHF/460 MHz, UHF-T/470 MHz, and UHF/800 MHz bands. Although there are still a considerable number of analog and conventional radio systems in use, more and more agencies are adopting other configurations (such as digital systems or trunked systems) as a result of modernization or mandates (for example, the FCC requires that all local and State public safety agencies move from wideband to narrow band configurations no later than December 31, 2013). As system operators migrate to modern infrastructure, many are also switching to systems that use IP technology to propagate signals.	❑ GATHER, COLLECT Radio systems may be used in emergencies by EMS providers to report crimes or incidents that they come upon during local travel or at incident scenes. Both dispatchers and EMS providers may use radios to gather descriptions or to request additional resources. ❑ ANALYZE Modern radio infrastructure may offer information systems that analyze capacity and call load for internal purposes, but such capabilities are not end user features. ❑ SHARE, COMMUNICATE, NOTIFY Radio infrastructure is routinely used by dispatchers and EMS providers to share, communicate, and notify. While voice communications make up the vast majority of traffic, some radio systems permit field forces to send urgent traffic via activation of an emergency switch located on the end user's radio to alert dispatchers when that user is at high risk and need immediate assistance. ❑ SERVE, RESPOND, OPERATE Radio infrastructure is a vital tool in the delivery of EMS. Personnel use radios to receive assignments, broadcast status changes, request resources, consult with online medical control, coordinate with mutual aid agencies, and provide situational awareness to their peers and supervisors. This cyber resource is critical to provider safety and patient care, providing an immediate means of reporting trouble and requesting assistance when they might otherwise be unable to access landline telephones. ❑ RECORD, SAVE, REVIEW Most EMS agencies use logging recorders to record all radio traffic in a given period, and they save these recordings for investigative and informational purposes and to support training and procedural improvements.
Tele-communications Services	EMS agencies use a variety of telecommunications services, from POTS to pagers, PDAs to smart phones, cellular telephones, ePCR devices, and ESMR to conduct and support interaction with the general public, coordinate investigative leads, and conduct administrative business. Although many agencies are still using original 1A2 keyset technology in their telephony, the use of IP-based and user friendly GUIs has begun to modernize the citizen-to-authority	❑ GATHER, COLLECT Call takers use POTS and IP-based or GUI-enhanced telephone systems to receive and process calls for dispatch and to make notifications to allied services such as fire and emergency services agencies or law enforcement. ❑ ANALYZE Telecommunications services generally are not

	communications. Under the provisions of the Americans with Disabilities Act, EMS communications centers are required to provide equal access to emergency telephone numbers and so they use TTY or other TDD to intercommunicate with the deaf and hard of hearing populations they serve.	used to analyze information, but the networks over which these services operate are often used for supporting software and connectivity with other agencies. A notable exception is Enhanced and Next Generation 9-1-1 services, which permit call takers in communications centers to receive ANI/ALI and analyze the data to verify the telephone numbers and addresses for callers. This simple analysis helps assure that EMS personnel are sent to the correct location every time. ❑ SHARE, NOTIFY, COMMUNICATE EMS agencies use telephony to place and receive calls, make notifications, conduct administrative business, and communicate with the public. Some ePCR systems provide EMS personnel with a tool to document patient information, medical signs and symptoms, and interventions taken to provide emergency medical care. In turn, these ePCR systems may use wireless telephony to transfer that data via facsimile to receiving hospitals, base agencies, billing services, and State health agencies. ❑ SERVE, RESPOND, OPERATE Telecommunications services are routinely used to serve the public to facilitate response of allied services (fire and emergency service agencies, law enforcement, etc.). ❑ RECORD, SAVE, REVIEW Telecommunications systems such as PDA devices and smartphones offer voice, data, and video capabilities that can capture and record images and information in a manner that can be retrieved or saved onto more permanent electronic data storage systems for future review. Enhanced and Next Generation 9-1-1 systems record the details of every call a communications center receives, such as date/time, ANI/ALI, times to answer, and duration of the call; which can be helpful in investigating complaints, substantiating reports of lost connectivity with telephone company switching offices, and addressing criminal acts. TTY and TDD systems use text messaging to communicate, which offers the option of printing records of conversations in much the same way that logging recorders collect voice traffic.

Emergency Management		
Cyber Technology/ Resource	**Description**	**Cyber Technology/Resource Application**

Geospatial Tools and Systems	Geospatial tools and systems include such resources as GIS databases, which contain critical infrastructure features such as utility placement, government facility types and locations, and property plats. They also include mapping data, services such as AVL to support more effective use of CAD systems, and situational awareness applications that permit end users, emergency managers, and government officials to see the deployments of resources for specific incidents or events. They may be used to display geospatial information to understand routes of travel and evacuation. They provide data to inform intelligence link analysis tools as well. Computer-aided drawing packages help emergency managers develop detailed displays of disaster impact areas and evacuation areas, highlighting the locations of critical infrastructure, public works and public utility easements, emergency shelters, or other features of interest.	❑ GATHER, COLLECT Geospatial systems permit emergency managers to gather and collect characteristics of a particular business or target hazard or disaster site, such as topology, proximity to public utility easements and transportation routes, and the layout of industrial campuses and parks, as well as evacuation routes and potential sites for emergency shelters and mass care. ❑ ANALYZE Emergency managers and others use GIS and geospatial tools to analyze the results of prior responses, to predict the likelihood of a recurrence of major incidents (such as floods, wildfires, or hazardous materials releases), or to predict when and where populations may head to when a disaster occurs. Examining these trends for commonalities and differences helps to inform planning, preparedness, and mitigation measures. These systems help decisionmakers, such as government officials, prioritize and fund these measures to reduce or eliminate community risk. They also help emergency managers determine where to put resources when considering issues such as transportation routes and means, at-risk populations, locations of target hazards, and potential sheltering locations. ❑ SHARE, COMMUNICATE, NOTIFY Once emergency preparedness strategies are developed, emergency managers can use geospatial systems and tools to share that data within their organization, with other dependent agencies in the same jurisdiction, or with other jurisdictions and agencies to create force multiplication in their efforts to effectively, efficiently, and safely respond to and recover from emergencies and disasters. ❑ SERVE, RESPOND, OPERATE Emergency managers use the products that geospatial tools and systems yield to make resource ordering decisions, develop mission assignments, predict resource deployments, support policy making, address legal considerations, and take steps to assure continuity of government. Geospatial tools and systems create products that help document impacts and losses, which can be vitally important when government officials must make decisions about declaring local, State, or even Presidential emergencies. ❑ RECORD, SAVE, REVIEW The same products used to support decision-

		making during the response phase of a disaster are used by emergency managers to help develop after action reports and provide justification for funding from local, State, or Federal disaster relief resources.
Internet	The Internet provides emergency managers with open sources for research that can be used to gain insights about emergencies occurring elsewhere to glean lessons learned, identify source materials for training, consider potential impacts on their own jurisdiction, or to learn about the factors that affected the people, processes, and technologies at the disaster site. They may also use the Internet to conduct outreach and deliver disaster preparedness education to the public. Tools such as social networking sites (Twitter®, Facebook®, MySpace®, and others) provide a means of readily communicating business, residential, and family preparedness tips, and updates on significant incidents. Many emergency management agencies use the Internet to provide official news and directions for the public in the event of an emergency.	❑ GATHER, COLLECT Emergency managers use the Internet to conduct open-source research that may help them learn about how major incidents in their region, in their State, or even around the world, are being addressed. They may also use database products such as the Responder Knowledge Base developed for the Web by DHS to learn about sources for tools, equipment, and other resources they may need for an incident they are overseeing. They may use Web applications or electronic mail to obtain information about people and businesses that need disaster relief in their areas of responsibility. They may also use social media to collect real-time data on immediate needs, and identify where people are in need of rescue or other urgent assistance. ❑ ANALYZE Social networking sites provide a variety of information about emergencies based on interaction between the agency and the public. Data on specific incidents and impacts can be analyzed to develop a strategy and tactical plan to address rescue operations, evacuations, shelters, relief efforts, distribution points, and recovery centers. ❑ SHARE, COMMUNICATE, NOTIFY The Internet provides agencies with the ability to interact with the public via electronic mail, social media sites, or Web pages to prevent, detect, and solve crimes. All emergency management agencies use the Internet to transmit and receive electronic mail for internal and external purposes. Social media has also been used by emergency management agencies to communicate the locations of disaster relief resources or to direct people to distribution centers. ❑ SERVE, RESPOND, OPERATE Many emergency management agencies possess computing resources that permit their staff leaders to send text messages or electronic mail while deployed in the field. These capabilities may tap regular telecommunications infrastructure or find connectivity by alternate means, such as satellite. This permits on-scene staff to interact with key government officials and decision makers to requisition resources or to direct relief

		operations from the incident site, if necessary. By policy, some emergency management agencies confine their work to the EOC. In those instances, Internet access is most often accomplished when in the EOC. ❑ RECORD, SAVE, REVIEW Some agencies permit the public to submit disaster claims via the Internet. Text messages via social media or other sources may or may not be saved for historical purposes, but may be reviewed to assure proper use of time and resources.
Public Alerting and Warning Systems	The emergency management community is the "power user" group of public alerting and warning systems. At their disposal, they use such systems as the EAS, emergency alert networks that disperse information to citizen subscribers via their registered devices (cellular telephones, pagers, electronic mail, etc.), sirens, and public address systems. Some agencies use Reverse 9-1-1® or similar products to send warnings to entire communities when the need arises.	❑ SHARE, NOTIFY, COMMUNICATE These systems use software that may be dependent on other cyber communications resources to disseminate their messages, such as telephony, telecommunications services, and the Internet. An example is a Reverse 9-1-1 system, which can be used to rapidly dial the home and business telephones in a defined segment of a community, an entire community, or even an entire jurisdiction to issue warnings such as "boil water orders" when a major public water distribution failure has occurred. Local, State, Federal, and tribal emergency management agencies have some level of access to EAS, whether it is with local television or radio broadcast stations or satellite and cable communications companies, or more. EAS is commonly used to alert the population to severe weather warnings, when evacuations may be ordered in response to flooding or HAZMAT emergencies, or to simply conduct tests to assure that the system is operational and capable of disseminating information when needed. ❑ SERVE, REPORT, OPERATE Public alerting and warning systems are used in real time to issue warnings, such as by activating sirens when a tornado is approaching a community. Public address systems may be used in downtown business districts or on college campuses, where significant pedestrian traffic in public areas make using loudspeakers to issue official news and directions a sensible option. ❑ RECORD, SAVE, REVIEW Some systems generate permanent records when they are used, while others do not.
Radio Infrastructure	Emergency management agencies use spectrum in the amateur, aviation, land mobile, and marine radio bands to coordinate with law enforcement, fire and emergency services, EMS, public works, public health, and	❑ GATHER, COLLECT Radio systems may be used to communicate with on-scene incident commanders and command posts to collect information on the

	transportation agencies in the event of a major emergency. Amateur radio is considered the last ditch means of continuity of communications, after all other forms of communications infrastructure has been lost. Many EOCs have access to mutual aid radio systems, statewide public safety radio networks, or other general government service radio systems to assure communications can continue while other systems such as telephone and the Internet may be unavailable. In the amateur radio bands, most EOC sites are equipped to access regular and proprietary radio systems in the VHF/low band, such as the Federal Emergency Management Agency's National Radio System. In the LMR band, they may operate in the VHF/high band and VHF/low band, in the UHF/460 MHz, the UHF-T Band/470-500 MHz, and UHF/800 MHz Bands. Although there are still a considerable number of analog and conventional radio systems in use, more and more agencies are adopting other configurations (such as digital systems or trunked systems) as a result of modernization or mandates (for example, the FCC requires that all local and State public safety agencies move from wideband to narrow band configurations no later than December 31, 2013). As system operators migrate to modern infrastructure, many are also switching to systems that use IP technology to propagate signal.	status of operations or unmet requirements. ❑ ANALYZE Modern radio infrastructure may offer information systems that analyze capacity and call load for internal purposes, but such capabilities are not end user features. ❑ SHARE, COMMUNICATE, NOTIFY Radio infrastructure is not used on a daily basis by most emergency managers, but when needed, it is used to share, communicate, and notify. ❑ SERVE, RESPOND, OPERATE Radio infrastructure is a critical component of continuity of communications in the emergency management community. Radio systems may be used to coordinate efforts and strategies among various area command posts or to direct and redirect resources as greater situational awareness is gained about an emergency or disaster. Radios may be used to report status changes, request resources, coordinate with mutual aid agencies, and provide situational awareness to government and decisionmaking officials present in an EOC. ❑ RECORD, SAVE, REVIEW Some EOC facilities use logging recorders on the various radio networks they use, but this is not a widespread practice.

Public Works		
Cyber Technology/ Resource	**Description**	**Cyber Technology/Resource Application**
Computer Aided Design and Drawing	Computer Aided Design and Drawing (CAD/D) systems provide critical detail and consistency for documenting the design elements of public works and critical infrastructure components from initial architecture through design, construction, assembly, and implementation phases, and contributing the baseline data needed for maintenance and operations of these works and components. CAD/D software packages typically interface with other data elements such as GIS and geospatial data information to create products that provide clear relationships between topological mapping and actual emplacement of public works and critical infrastructure components. Programs such as Auto-CAD® are frequently used by public works engineers, as they	❑ GATHER, COLLECT CAD/D systems help engineers create both 2-D and 3-D renderings of civil infrastructure and infrastructure network layouts, such as water and sewer system mapping and imaging. These software packages help public works officials show linkages between infrastructure systems as well as the core system components to other agencies or to end users in communities. ❑ RECORD, SAVE, REVIEW Public works engineers and system operators record and save updates to official drawings and records to show changes in infrastructure networks and elements based on previous renderings.

	support easily portrayed civil infrastructure, such as water pipelines and building infrastructure, and can be manipulated to produce both two- and three-dimensional (2-D and 3-D) drawings.	
Geospatial Tools and Systems	Geospatial tools and systems include such resources as GIS databases, which contain critical infrastructure features such as utility placement, government facility types and locations, and property plats. They may also include mapping data, services such as AVL to support more effective use of mobile resources, and situational awareness applications that permit end users, dispatchers, and supervisors to see the deployments of resources for specific incidents or events. They may be used to provide field forces with navigational aids, or provide dispatchers with a display of geospatial information to understand routes of travel and escape. They provide data to inform intelligence link analysis tools as well.	❑ GATHER, COLLECT Geospatial systems permit public works agencies to gather and collect characteristics of trouble locations, dates, times, and weather, rights-of-way and easement data, and shared infrastructure placements that may require coordination with other agencies or organizations. ❑ ANALYZE Public works officials and engineers can analyze the data to predict when and where the consequences of incidents such as sewage breaks, water main breaks, or other failures in publicly maintained pipelines are reported to develop strategies that can be used to reroute services, resolve the effects of effluent losses, and identify communities that may be required to take action such as evacuation, shelter in place, boil water, or follow other directions. ❑ SHARE, COMMUNICATE, NOTIFY Once strategies are developed, public works agencies can use geospatial systems and tools to share that data within their organization or with other jurisdictions and agencies to create force multiplication in their efforts at locating, confining, and resolving systemic failures or pipeline breaks. ❑ SERVE, RESPOND, OPERATE Public works agencies use the products that geospatial tools and systems yield to effect resource deployments, detect patterns and practices associated with infrastructure failures, respond more effectively, and operate more safely based on increased situational awareness. ❑ RECORD, SAVE, REVIEW Products of geospatial tools and systems can be retained to locate easements or rights-of-way information, and provide a geographic history to inform modernization or retrofit plans and financing. Systems such as AVL are used in real time to inform resource response recommendations or to help dispatchers gain situational awareness about deployed resources to manage gaps in coverage, or locate personnel or vehicles that are otherwise out of communication.
Internet	The Internet provides public works agencies with open sources for research that can be	❑ GATHER, COLLECT

	used to operate Web tools, conduct outreach, and inform the public. Tools such as social networking sites (Twitter®, Facebook®, MySpace®, and others) provide a means of readily communicating critical infrastructure and traffic updates and providing official news and directions for end users in the event of an emergency.	Public works agencies use the Internet to conduct open-source research that may help them identify traffic accident locations, locate disabled vehicles or other obstacles blocking roadways, collect real-time traffic and critical infrastructure tips from the public, or even learn about problems that have not yet been officially reported. ❑ ANALYZE Social networking sites provide a variety of information about real-time traffic incidents, those yet to be officially reported or investigated, and those whose impacts are continuing to expand or increase. Specialists can analyze images and video captured by IP-based camera and traffic monitoring posts with citizen reports and incident responses from law enforcement, fire and emergency services, or EMS to identify sources of congestion or tie-ups to offer detours or to direct response resources more effectively to resolve problems faster. ❑ SHARE, COMMUNICATE, NOTIFY The Internet provides agencies with the ability to interact with the public via electronic mail, social media sites, or Web pages. Many agencies encourage electronic reporting of instances of infrastructure failures or damage to any public works, and also to provide a means of reaching senior officials to offer compliments or complaints. Nearly all public works agencies use the Internet to transmit and receive electronic mail for internal purposes. ❑ SERVE, RESPOND, OPERATE Many public works agencies provide computing resources that permit their personnel to send text messages or electronic mail while deployed in the field or in quarters, depending on agency policies. ❑ RECORD, SAVE, REVIEW Some agencies permit the public to submit correspondence via the Internet that can be saved for an official response. Text messages may not be saved for historical purposes, but may be reviewed to assure proper use of time and resources.
Radio Infrastructure	Public works agencies use spectrum in the government services and LMR bands to conduct administrative business, support deployed mobile resources, maintain connectivity between public safety and public works facilities, or to conduct RF monitoring of supervisory devices at sites such as dams, reservoirs, and maintenance shops. In the LMR band alone, they operate in both the	❑ GATHER, COLLECT Radio systems may be used in public works agencies to investigate infrastructure losses or damages and to report findings. Supervisory systems are popular in public works agencies that operate water collection, treatment, purification, and distribution systems for collecting data from scientific and industrial

	VHF/high band and VHF/low band, and in the UHF band. Although there are still a considerable number of analog and conventional radio systems in use, more and more agencies are adopting other configurations (such as digital systems) as a result of modernization or mandates (for example, the FCC requires that all local and State public safety agencies move from wideband to narrow band configurations no later than December 31, 2013). As system operators migrate to modern infrastructure, many are also switching to systems that use IP technology.	monitoring equipment. ❑ ANALYZE Modern radio infrastructure may offer information systems that analyze capacity and call load for internal purposes, but such capabilities are not end user features. ❑ SHARE, COMMUNICATE, NOTIFY Radio infrastructure is routinely used to share, communicate, and notify dispatchers and public works crews and facilities. Although voice communications make up the vast majority of traffic, some applications send data only and are used to monitor the status of critical infrastructure facilities. ❑ SERVE, RESPOND, OPERATE Radio infrastructure serves to provide more effective public works operations. Crews use radios to receive assignments; broadcast status changes; request resources; check on restoration reports, breaks, and related outages; and provide situational awareness to their peers and supervisors. This cyber resource is important to public works command and control centers that monitor critical infrastructure or traffic control systems, and that interact with public safety command, control, and communications centers. ❑ RECORD, SAVE, REVIEW Most public works agencies do not use logging recorders to record voice radio traffic in a given period, although they may have recordings of data transmissions. These recordings play an important role in maintaining proper operating conditions and aid in investigative and informational purposes to learn the events behind a loss or interruption of services, or to support training and procedural improvements.
Security and Surveillance Systems	Public works agencies that monitor critical infrastructure facilities routinely incorporate security and surveillance systems to accomplish those missions. Public works dispatchers or engineers receive and interpret activations of security alarm systems at public works sites and facilities. Such systems may be passive (such as security systems arranged to detect intrusion through windows and doors via a wide array of technology, or data monitoring systems that send status information on a regular cycle) or active (designed to be manually activated, such as the alarms that site operators may trip when a major system fails or a dam breaks). The systems usually trigger audible alarms (which may or may not include visual signals such as warning lamps to draw operator attention to	❑ GATHER, COLLECT Security and surveillance systems may have the ability to record audio and/or video at protected premises. ❑ ANALYZE These systems generally do not offer analytical capabilities, but may provide data that can be analyzed at a later time. ❑ SHARE, COMMUNICATE, NOTIFY Security and surveillance systems may offer connectivity to transmit activations to monitoring stations for review and action. Some systems include annunciation information that permits field forces to know the type of alarm activated (manual or automatic, supervisory or urgent) and

	the activation), depending on the premises protected. Some security systems also include supervisory features to detect tampering with system components or connectivity lines. Some systems may be local systems that do not transmit activations to monitoring (central stations) services, as they may be intended only to serve as reminders or prompts to cause public works employees to take a specific action. Public works agencies may rely on security systems to protect isolated or sensitive locations, such as property yards, water treatment plants, or radio tower sites. Public works agencies may also operate surveillance systems that permit them to use cameras and closed circuits to observe activities in high-risk infrastructure areas, major traffic congestion areas, dangerous industrial processing or materials storage areas, or their own offices and garage facilities, and parking lots.	location. ❑ SERVE, RESPOND, OPERATE Live surveillance systems that are monitored through a closed circuit can help dispatchers to direct field forces to broken infrastructure, traffic snarls, or lost connections with public works sites to investigate the cause and recommend or take action. They can also help dispatchers understand whether fires, explosions, HAZMAT releases, or personal injuries have been incurred to prompt them to send emergency services with public works crews. ❑ RECORD, SAVE, REVIEW Many surveillance systems include either hard or soft recording media that can be retrieved for analysis and that can become part of the case record for a given crime. Products such as video recordings can be instrumental in determining the extent of damage or loss, and in planning restoration or reconstitution of services.
Tele-communications Services	Public works agencies use a variety of telecommunications services, from POTS to pagers, PDA to smartphones, cellular telephones, and ESMR to conduct and support interaction with the general public, coordinate resources, and conduct administrative business. Although many agencies are still using original 1A2 keyset technology in their telephony, the use of IP-based and user-friendly GUIs has begun to modernize the citizen to authority communications. Other systems may include VMBs to communicate warnings, such as advising motorists about checkpoints ahead, or to issue Amber or Silver Alerts.	❑ GATHER, COLLECT Call takers use POTS and IP-based or GUI-enhanced telephone systems to receive and process calls for dispatch and to make notifications to allied services such as fire and rescue, law enforcement agencies, public utilities, etc. ❑ ANALYZE Telecommunications services generally are not used to analyze information, but the networks over which these services operate are often used for supporting software and connectivity with other agencies. ❑ SHARE, NOTIFY, COMMUNICATE Public works agencies use telephony to place and receive calls, make notifications, conduct administrative business, and communicate with the public. ❑ SERVE, RESPOND, OPERATE Telecommunications services are routinely used to serve the public and facilitate response of allied services (power companies, tree trimmers, etc.). Devices such as VMBs may be used to support special or long-term operations and disaster response and recovery. ❑ RECORD, SAVE, REVIEW Telecommunications systems such as PDA devices and smartphones offer voice, data, and video capabilities that can capture and record images and information in a manner that can be retrieved or saved onto more permanent

		electronic data storage systems for future review.
Watch and Warning Systems	Public works agencies use fixed and portable watch and warning systems, such as VMBs, to communicate warnings, such as advising motorists about road hazards, changes in traffic patterns, boil water alerts, or as a service to allied agencies, such as law enforcement, to warn motorists of checkpoints ahead, or to issue Amber or Silver Alerts. Some agencies use Reverse 9-1-1® or similar products to send warnings to entire communities when the need arises.	❑ SHARE, NOTIFY, COMMUNICATE These systems use software that may be dependent on other cyber communications resources to disseminate their messages, as is the case with fixed VMB devices. In many cases, neither Amber nor Silver Alerts to notify the public to locate missing and endangered juveniles and elderly adults are software packages; they simply use VMB systems as the means to convey messages. ❑ SERVE, REPORT, OPERATE Devices such as VMBs may be used to support special or long-term operations and disaster response and recovery. ❑ RECORD, SAVE, REVIEW These systems are used to support public works operations but they generally do not record or save the data disseminated for later review.

Public Safety Communications and Coordination/Fusion		
Cyber Technology/ Resource	**Description**	**Cyber Technology/Resource Application**
Computer Aided Dispatch	CAD systems combine the power of personal computing and mainframe computing to draw data from criminal justice databases, motor vehicle administration databases, GIS, police, fire, and EMS resource deployment plans, ANI and ALI records provided by POTS providers, and callers seeking law enforcement, fire, emergency service, and EMS assistance. CAD systems give dispatchers and call takers the ability to receive telephone calls from the public, quickly determine the origin of the call, ascertain the nature of the need for assistance, and transmit processed requests in a fraction of the time required if this task was performed manually. On demand, dispatchers can query the system about processed requests that are pending action and seek a recommendation from the system on the most appropriate response for each request. If the dispatcher agrees, the request is quickly transmitted via wireless connection to field forces available.	❑ GATHER, COLLECT CAD systems are used to gather information from callers and field forces, and to collect the data in a useable form ❑ ANALYZE CAD systems analyze the data and develop response recommendations. The dispatcher can seek a recommendation, agree, and transmit the recommendation. Alternatively, the dispatcher can disagree and dispatch resources based on his/her own recommendations. ❑ SHARE, COMMUNICATE, NOTIFY CAD systems permit end users to share the data among end users who have access to query the information. They support data communications such as text messaging between end users and dispatchers. They permit dispatchers to send assistance when more resources are needed. ❑ SERVE, RESPOND, OPERATE End users use CAD terminals to acknowledge the dispatch of resources, indicate their responses, and notify others of their arrival using status changes in the system, which automatically records

		associated times and event numbers for each request. End users can then use the CAD terminal in the communications center or in their vehicles during the course of operating on the scene of an incident to query various databases and research history for a particular address or incident. ❑ RECORD, SAVE, REVIEW End users add text to enhance the geospatial and public safety knowledge about the premises involved in incidents. The end results are retained for criminal justice purposes, to inform planning and research activities for improved resource deployment, reduced response times, and justified increases or decreases in resource allocations. Some CAD systems also offer RMSs capable of supporting not just CAD records but incident reporting software, including national incident reporting system-compliant software, that permits either over-the-air submission or external drive and hard disk downloads to desktop terminals at stations.
Criminal Justice Networks and Systems	There are a variety of local, State, and Federal criminal justice networks and services that the public safety communications staff uses around the clock. These networks, and the services they provide, are located on private wired and wireless terminals and connections. NLETS serves as the backbone for a private network that links all local, State, and many Federal law enforcement agencies for the purposes of communicating criminal justice information and sharing access to criminal justice databases. The most well-known and -used service is the NCIC, a database resource created, maintained, and operated by the FBI to collect and share criminal justice information about wanted and missing persons, and lost and stolen property, such as guns, vehicles, and other goods. The FBI requires that all law enforcement and public safety communications personnel that access NCIC complete a rigorous training and certification program regularly, that terminals and their locations are restricted to prevent unauthorized use or access, and that access terminals be used solely for criminal justice purposes; they are expressly prohibited from connection with the Internet or other non-law enforcement network or communications system.	❑ GATHER, COLLECT Criminal justice networks provide a repository for victim and witness information, contacts by law enforcement officers with the public, criminal history, the existence and status of warrants for arrest, the names and descriptions of persons missing or wanted, and the makes, models, serial numbers, and descriptions of lost and stolen articles. Public safety communications staff frequently uses these systems to verify the existence and location of a warrant when a law enforcement officer in the field locates someone who may be wanted. ❑ ANALYZE Most public safety communications agencies support investigations by making queries to search for relevant data in a criminal justice database, but the actual analysis is done separately. ❑ SHARE, COMMUNICATE, NOTIFY Criminal justice networks and systems provide the ability for agencies to send inquiries to other law enforcement and public safety communications agencies in their region, their State, or nationwide to seek information about crimes that may indicate a larger pattern of incidence, or perpetrator(s) operating in more than one jurisdiction. Agencies can share data, notify surrounding agencies to be on the lookout for wanted persons or vehicles involved in crimes, and notify other agencies of the occurrence of major crimes or disasters that may require force multiplication to conduct searches, manhunts, or urgent response. ❑ SERVE, RESPOND, OPERATE

		Public safety communications staff may be asked by law enforcement officers to use a criminal justice system to query a database, or they may have access to CAD terminals from which they can conduct their own queries. Public safety communications staff may receive and process such requests dozens of times in a work period, depending on the number of field forces they are supporting. Generally, field forces make these requests while on patrol, when they encounter suspicious people or vehicles or while they are on the scene of a crime and need sensitive information to support their investigation. ❑ RECORD, SAVE, REVIEW On behalf of law enforcement officers they serve, public safety agencies routinely enter, modify, and withdraw entries from various database using criminal justice systems and networks. NCIC, for example, requires that the State police agency in every State conduct audits of the local, State, and tribal law enforcement agencies with access to that system, to assure that only staff members who are trained, certified, and authorized are accessing the system, that record keeping is organized and up-to-date, and that all entries meet FBI criteria, with all exceptions purged from the system to maintain the quality and integrity of the system.
Geospatial Tools and Systems	Geospatial tools and systems include such resources as GIS databases, which contain critical infrastructure features such as utility placement, government facility types and locations, and property plats. They also include mapping data, services such as AVL to support more effective use of CAD systems, and situational awareness applications that permit end users, dispatchers, and supervisors to see the deployments of resources for specific incidents or events. These tools and systems may be used to provide field forces with navigational aids or provide dispatchers with a display of geospatial information to understand routes of travel and escape. They provide data to inform intelligence link analysis tools as well. Computer-aided drawing packages help victims and witnesses to identify criminal perpetrators through software packages that can create sketches in the absence of photographs.	❑ GATHER, COLLECT Geospatial systems permit communications and coordination groups (such as law enforcement agencies, homeland security agencies, emergency management agencies, and public safety communications agencies) to gather and collect characteristics of a crime, such as victims, witnesses, suspects, lookouts, weapons used, articles taken, locations, dates, times, and weather. ❑ ANALYZE Communications and coordination groups, operating in a consolidated fusion center environment, analyze the data to predict when and where future crimes or terrorist acts may occur to develop strategies that can be used to prevent, detect, deter, or disrupt such acts, or to solve cases involving actual events and convict the offenders involved. These groups review data to detect links among people, places, and events. These strategies and the tactics developed to support them, help prevent, detect, disrupt, and deter homeland security threats. ❑ SHARE, COMMUNICATE, NOTIFY These systems and tools can be used to share data internally or with other jurisdictions and agencies to create force multiplication in their efforts to predict, detect, and locate crimes, and arrest criminal offenders. Such communications

		may also be used to populate intelligence linking systems to detect other commonalities. ❑ SERVE, RESPOND, OPERATE Products that geospatial systems and tools yield are used in fusion centers to effect resource deployments, conduct patrol patterns and practices, respond more effectively, and operate more safely based on increased situational awareness. ❑ RECORD, SAVE, REVIEW These systems and tools can be retained to locate articles or materials of evidentiary value and provide a geographic history to inform crime trends and help plan crime prevention and detection measures. Systems such as AVL are used in real time to inform public safety communications staff. These systems support CAD system response recommendations and help dispatchers gain situational awareness about deployed resources to better manage gaps in coverage, to locate personnel or vehicles that are otherwise out of communication, or to help in planning break times for field forces.
Intelligence Link Analysis Tools and Systems	Communications and coordination groups, particularly those operating in a fusion center environment, use such tools and systems to plot the sites of criminal or suspicious activities to detect patterns of practice and learn about methods of criminal operation that can aid investigators in developing suspects or predicting where future crimes or terrorist acts may occur.	❑ GATHER, COLLECT These systems and tools permit law enforcement agencies and fusion centers to gather geospatial information and collect characteristics of a suspicious event or a crime, such as victims, witnesses, suspects, lookouts, weapons used, articles taken, locations, dates, times, and weather. ❑ ANALYZE Analysts or investigators analyze data to seek commonalities, identify suspects, detect patterns, or predict when and where future crimes may occur to develop strategies and tactics that can be used to solve cases and convict criminal offenders. They may also use the results of analysis to inform strategy and tactics development to prevent, detect, disrupt, or deter terrorist acts. ❑ SHARE, COMMUNICATE, NOTIFY These systems and tools are used to share that data within a fusion center environment, within an organization, or with other jurisdictions and agencies to create force multiplication in efforts at predicting, detecting, and locating crimes; arresting criminal offenders; or preventing, detecting, disrupting, or deterring terrorist acts. ❑ SERVE, RESPOND, OPERATE Products that geospatial systems and tools yield are used to effect resource deployments, conduct patrol patterns and practices, respond more effectively, and operate more safely based on

		increased situational awareness. ❑ RECORD, SAVE, REVIEW Products of geospatial systems and tools can be retained to rule in or rule out suspects, locate articles or materials of evidentiary value, and provide a history to inform crime trends and help plan crime or terrorism prevention and detection measures. Systems such as AVL are used in real time to inform CAD system response recommendations or to help dispatchers gain situational awareness about deployed resources to manage gaps in coverage, locate personnel or vehicles that are otherwise out of communication, or allow break times for field forces.
Internet	The Internet provides public safety communications and coordination groups with open sources for research that can be used to detect and locate suspects, track criminal information offers, conduct outreach, and inform the public. Tools such as social networking sites (Twitter®, Facebook®, MySpace®, and others) provide a means of readily communicating crime prevention tips, witness and suspect information, and providing official news and directions for end users in the event of an emergency.	❑ GATHER, COLLECT The Internet is used to conduct open-source research that may help them identify suspects, locate missing or wanted persons, collect crime-solving tips, or even learn about crimes that have not yet been officially reported. ❑ ANALYZE Social networking sites provide a variety of information about crimes and suspects, from incidents yet to be officially reported or investigated, to suspects posting stories or bragging about their exploits online. Computer forensic specialists can then analyze content and work with Internet service providers to locate the originating computers to find missing or wanted persons. ❑ SHARE, COMMUNICATE, NOTIFY The Internet provides agencies with the ability to interact with the public via electronic mail, social media sites, or Web pages to prevent, detect, and solve crimes. Many agencies encourage electronic reporting of instances of abuse of authority or excessive force by their officers, and also to provide a means of reaching senior officials to offer compliments or complaints. Nearly all public safety communications and coordination groups use the Internet to transmit and receive electronic mail for internal purposes. ❑ SERVE, RESPOND, OPERATE Many coordination groups provide computing resources that permit team members to send text messages or electronic mail while deployed in the field, but just as many agencies either prohibit it or only permit members with personally owned devices to use them on duty. Thus, for those groups, Internet access is most often accomplished when in quarters. The public safety communications staff often has restrictions on Internet access because of call volume, or exclusive use of terminals for access to criminal

		justice networks, which often prohibit connectivity with any outside resource not in the official network. ❑ RECORD, SAVE, REVIEW Some agencies permit the public to submit correspondence via the Internet that can be saved for an official response. Text messages may not be saved for historical purposes, but may be reviewed to assure proper use of time and resources.
Radio Infrastructure	Public safety communications agencies use spectrum in the aviation, land mobile, and marine radio bands to support field forces that may be engaged in patrol, response, search, rescue, and medical evacuation operations. In the LMR band alone, they operate in both the VHF/high band and VHF/low band, and in the UHF/460 MHz, UHF-T/470 MHz, and UHF/800 MHz bands. Although there are still a considerable number of analog and conventional radio systems in use, more and more agencies are adopting other configurations (such as digital systems or trunked systems) as a result of modernization or mandates (for example, the FCC requires that all local and State public safety agencies move from wideband to narrow band configurations no later than December 31, 2013). As system operators migrate to modern infrastructure, many are also switching to systems that use IP technology to propagate signal.	❑ GATHER, COLLECT In emergencies, radio infrastructure is used by public safety communications dispatchers to receive traffic from law enforcement officers reporting crimes or incidents that they come upon during patrol. Both dispatchers and officers may use radios to gather descriptions broadcast via lookouts. Dispatchers also gather situation reports to help support decisionmaking. ❑ ANALYZE Modern radio infrastructure may offer information systems that analyze capacity and call load for internal purposes, but such capabilities are not end user features. ❑ SHARE, COMMUNICATE, NOTIFY Radio infrastructure is routinely used by dispatchers and field forces (including law enforcement officers, firefighters, emergency service personnel, and EMS providers) to share, communicate, and notify. Although voice communications make up the vast majority of traffic, some radio systems permit field forces to send urgent traffic via activation of an emergency switch located on the end user's radio to alert dispatchers when that user is at high risk and need immediate assistance. ❑ SERVE, RESPOND, OPERATE Radio infrastructure is the backbone of public safety communications operations. Dispatchers use radios to send law enforcement officers, firefighters, emergency service personnel, and EMS providers to assignments; broadcast status changes; process requests for resources; report on the results of checks for wanted persons; and learn and provide situational awareness for their peers and supervisors. This cyber resource is critical to officer safety, providing an immediate means of reporting trouble and requesting assistance. It promotes prompt response and the continual awareness of deployed resources and their status. ❑ RECORD, SAVE, REVIEW Most public safety communications agencies use

		logging recorders to record all radio traffic in a given period, and they save these recordings for investigative and informational purposes and to support training and procedural improvements.
Surveillance Systems	Communications and coordination groups, especially those operating within a fusion center environment, may operate surveillance systems that permit them to use cameras and closed circuits to observe activities (including people and vehicles) in high-crime areas, high-security areas, at target hazard locations, or their own facilities, including hallways and parking lots. Some public safety communications centers may also provide limited central station monitoring for internal safety and security systems.	❑ GATHER, COLLECT Surveillance systems may have the ability to record audio and/or video at protected premises. ❑ ANALYZE These systems generally do not offer analytical capabilities, but may provide data that can be analyzed at a later time. ❑ SHARE, COMMUNICATE, NOTIFY Surveillance systems may offer connectivity to transmit data and images or streaming video to monitoring stations for review and action. Security systems may provide information such as location and type of alarm activated, and whether the alarm is manually activated (such as by pull station or switch) or automatically activated (such as by breaking entry through a door or window, or water flowing in a fire suppression sprinkler system). ❑ SERVE, RESPOND, OPERATE Live surveillance systems monitored through a closed circuit can help dispatchers to direct field forces to broken windows, points of entry, and even the direction that fleeing suspects may be leaving. They can also help dispatchers understand whether personal injuries have been incurred to prompt them to send EMS with law enforcement. ❑ RECORD, SAVE, REVIEW Many surveillance systems include either hard or soft recording media that can be retrieved for analysis and that can become part of the case record for a given crime. Products such as video recordings can be instrumental in criminal prosecution and determination of guilt.
Telecommunications Services	Public safety communications agencies use a variety of telecommunications services, from POTS to pagers, PDAs to smartphones, cellular telephones, and ESMR to conduct and support interaction with the general public, crime victims, and witnesses; coordinate investigative leads; and conduct administrative business. Although many agencies are still using original 1A2 keyset technology in their telephony, the use of IP-based and user-friendly GUIs has begun to modernize the citizen-to-authority and authority-to-citizen (such as Reverse 9-1-1®) communications. Under the provisions of the Americans with Disabilities Act, law enforcement communications centers are required to provide equal access to emergency telephone	❑ GATHER, COLLECT Call takers use POTS and IP-based or GUI-enhanced telephone systems to receive and process calls for dispatch and to make notifications to allied services such as law enforcement, fire and rescue, towing companies, public utilities, etc. ❑ ANALYZE These services are generally not used to analyze information, but the networks over which these services operate are often used for supporting software and connectivity with other agencies. A notable exception is Enhanced and Next Generation 9-1-1 services, which permit call takers in communications centers to receive ANI/ALI and analyze the data to verify the telephone numbers

	numbers and so they use TTY or other TDD to intercommunicate with the deaf and hard of hearing populations they serve. Data exchange hubs may be used to link telecommunications systems to support automatic and mutual aid, broad criminal investigations, or for administrative messaging and other interagency communications over data or video systems. Other systems may include VMBs to communicate warnings, such as advising motorists about checkpoints ahead, or to issue Amber or Silver Alerts.	and addresses for callers. This simple analysis helps assure that law enforcement field forces are sent to the correct location every time. ❑ SHARE, NOTIFY, COMMUNICATE Telephony is used to place and receive calls, make notifications, conduct administrative business, and communicate with the public. Some agencies are interconnected with data exchange hubs to permit communications among criminal justice networks, administrative messaging systems, CAD systems, or other telecommunications resources used by other agencies in the same functional area, in different functional areas, or across levels of government. ❑ SERVE, RESPOND, OPERATE Telecommunications systems are used to serve the public to facilitate response of allied services (tow trucks, power companies, medical examiners, etc.). Devices such as a fixed VMB may be used to support special or long-term operations and disaster response and recovery. ❑ RECORD, SAVE, REVIEW Telecommunications systems such as PDA devices and smartphones offer voice, data, and video capabilities that can be used to capture and record images and information in a manner that can be retrieved or saved onto more permanent electronic data storage systems for future review. Enhanced and Next Generation 9-1-1 systems record the details of every call a communications center receives, such as date/time, ANI/ALI, times to answer, and duration of the call, which can be helpful to investigating complaints, substantiating reports of lost connectivity with telephone company switching offices, and criminal acts. TTY and TDD systems use text messaging to communicate, which offers the option of printing records of conversations in much the same way that logging recorders collect voice traffic.
Watch and Warning Systems	Public safety communications agencies most commonly use systems such as Reverse 9-1-1 for alerting the public, although social media are being more widely adopted in the community. Legislation passed in the last few years have created new cyber venues for public alerting by law enforcement—Amber Alerts and Silver Alerts. Public safety communications staff supporting law enforcement agencies may be tasked with developing and disseminating Amber or Silver Alerts on their behalf.	❑ SHARE, NOTIFY, COMMUNICATE Software that is dependent on other cyber communications resources is used facilitate dissemination of alerting messages. In many cases, neither Amber nor Silver Alerts to notify the public to locate missing and endangered juveniles and elderly adults are software packages; they simply use TTY and VMB systems to convey messages. ❑ SERVE, REPORT, OPERATE Devices such as VMB may be used to support special or long-term operations and disaster response and recovery. ❑ RECORD, SAVE, REVIEW

	These systems are used to support emergency services efforts but they generally do not record or save the data disseminated for later review.

Appendix B: Emergency Services Sector Acronym List

2-D/3-D	Two Dimensional/Three Dimensional
ALI	Automatic Location Identification
ANI	Automatic Number Identification
AVL	Automatic Vehicle Location
BIM	Base Interface Module
CAD	Computer Aided Dispatch
CAD/D	Computer Aided Design and Drawing
CARMA	Cybersecurity Assessment and Risk Management Approach
CCTV	Closed-Circuit Television
DHS	Department of Homeland Security
EAS	Emergency Alert System
EMS	Emergency Medical Services
EOC	Emergency Operations Center
ePCR	Electronic Patient Care Reporting
ESMR	Enhanced Special Mobile Radio
ESS	Emergency Services Sector
ESS-CRA	Emergency Services Sector Cyber Risk Assessment
FCC	Federal Communications Commission
FBI	Federal Bureau of Investigation
GUI	Graphical User Interface
GIS	Geographical Information System
HAZMAT	Hazardous Material
IP	Internet Protocol
IT	Information Technology
LEA	Law Enforcement Agency
LMR	Land Mobile Radio
MHz	Megahertz
NCIC	National Crime Information Center
NCSD	National Cyber Security Division
NEMSIS	National Emergency Medical Services Information System

NGO	Non-Governmental Organization
NLETS	National Law Enforcement Telecommunication System
NIPP	National Infrastructure Protection Plan
NOC	National Operations Center
PASS	Personal Alert Safety Systems
PDA	Personal Digital Assistant
POTS	Plain Old Telephone System
PSC&C	Public Safety Communication and Coordination
RF	Radio Frequency
RMS	Records Management System
SANS	SysAdmin, Audit, Network, Security
SCBA	Self Contained Breathing Apparatus
SME	Subject Matter Expert
SQL	Structured Query Language
SSP	Sector-Specific Plan
SWAT	Special Weapons And Tactics
TDD	Telecommunication Device for the Deaf
TTY	Teletype
UHF	Ultra High Frequency
VHF	Very High Frequency
VMB	Variable Message Board
WPS	Wireless Priority Service

245 Murray Lane SW Bldg 410
Mailstop 0640
Washington DC 20528

essteam@hq.dhs.gov