Assessing National-Level Cyber Risk:
Threat Scenarios in the Emergency Services Sector

GFIRST Conference

Critical Infrastructure Protection Cyber Security (CIP CS) Program
National Cyber Security Division (NCSD)
Office of Cybersecurity and Communications
Department of Homeland Security

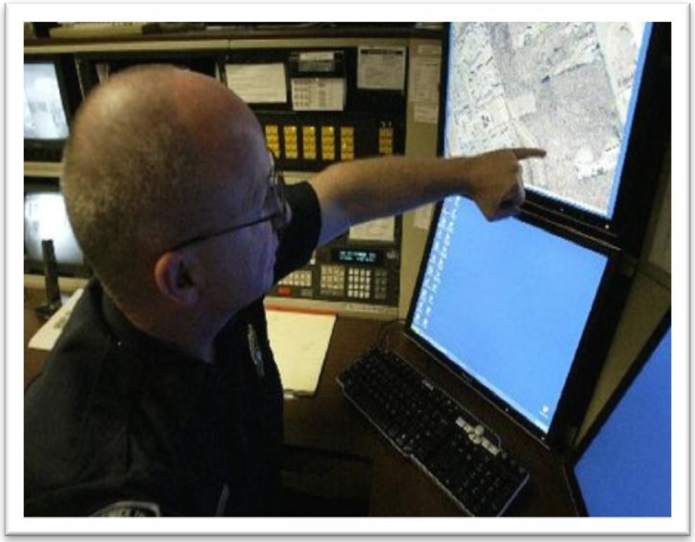
August 23, 2012

Homeland
Security

Agenda

- The Emergency Services Sector's need for a sector-level risk analysis
- Overview of the Cybersecurity Assessment and Risk Management Approach (CARMA)
- The Emergency Services Sector Cyber Risk Assessment
- Next steps and emerging issues

The Emergency Services Sector (ESS) depends on cyber infrastructure and faces a wide variety of cyber threats



- Over the past 10 years, ESS has become increasingly dependent on cyber assets, systems, and disciplines
- ESS faces risks from natural hazards and malicious actors including criminals, hackers, terrorists, and nation-states
- Although existing capabilities mitigate some threats, ESS still faces sector-wide risks to its ability to operate during emergencies
- Because of increasing dependence on cyber technology and the evolving threat landscape, assessing vulnerabilities and consequences is difficult
- ESS leadership identified the need for a collaborative framework to enhance sector resiliency and security

Recent cyber threats to ESS come from manmade deliberate, manmade unintentional, and natural causes

- “Lemont police suspect that someone hacked into the village’s tornado siren system, causing all seven sirens to sound for about 30 minutes, Police Chief Kevin Shaughnessy said today.”
  - *July 3, Chicago Tribune* – (Illinois) **Police: Hacker may have targeted Lemont’s tornado sirens.**

- “Hacktivists from the online group Anonymous claim to have taken down the Chicago Police Department's Web site in the wake of violent clashes between the police and protesters.”
  - *May 20, Wired*– (National) **Hacktivists claim takedown of Chicago police Web site.**

- “A critical computer network is down after falling victim to a sophisticated worm Friday, that system is down for the third day, impacting about 200 different agencies, including police departments, jails and courts all over northwest Ohio.”
  - *February 24, National Cyber Security* – (National) **NORIS computer system shut down over virus.**

- “The Washington D.C. government has temporarily halted use of one of its most popular Twitter accounts to get a tighter handle on information disseminated about emergency operations….”
  - *September 22, 2011, Washington Times* – (District of Columbia) **D.C. temporarily halts fire, EMS Twitter account.**

The Cybersecurity Assessment and Risk Management Approach (CARMA) brought together ESS jurisdictions in 2011 to strategically address cyber risk

Process

- Recruited members from all ESS disciplines to work to identify, prioritize, and manage cyber risks
- CARMA solicited input on widely impactful nationwide threats, vulnerabilities, and consequences through seven targeted evaluation sessions and scenarios
- CARMA's flexibility addressed the ESS' public-service mission to protect citizens and other sectors

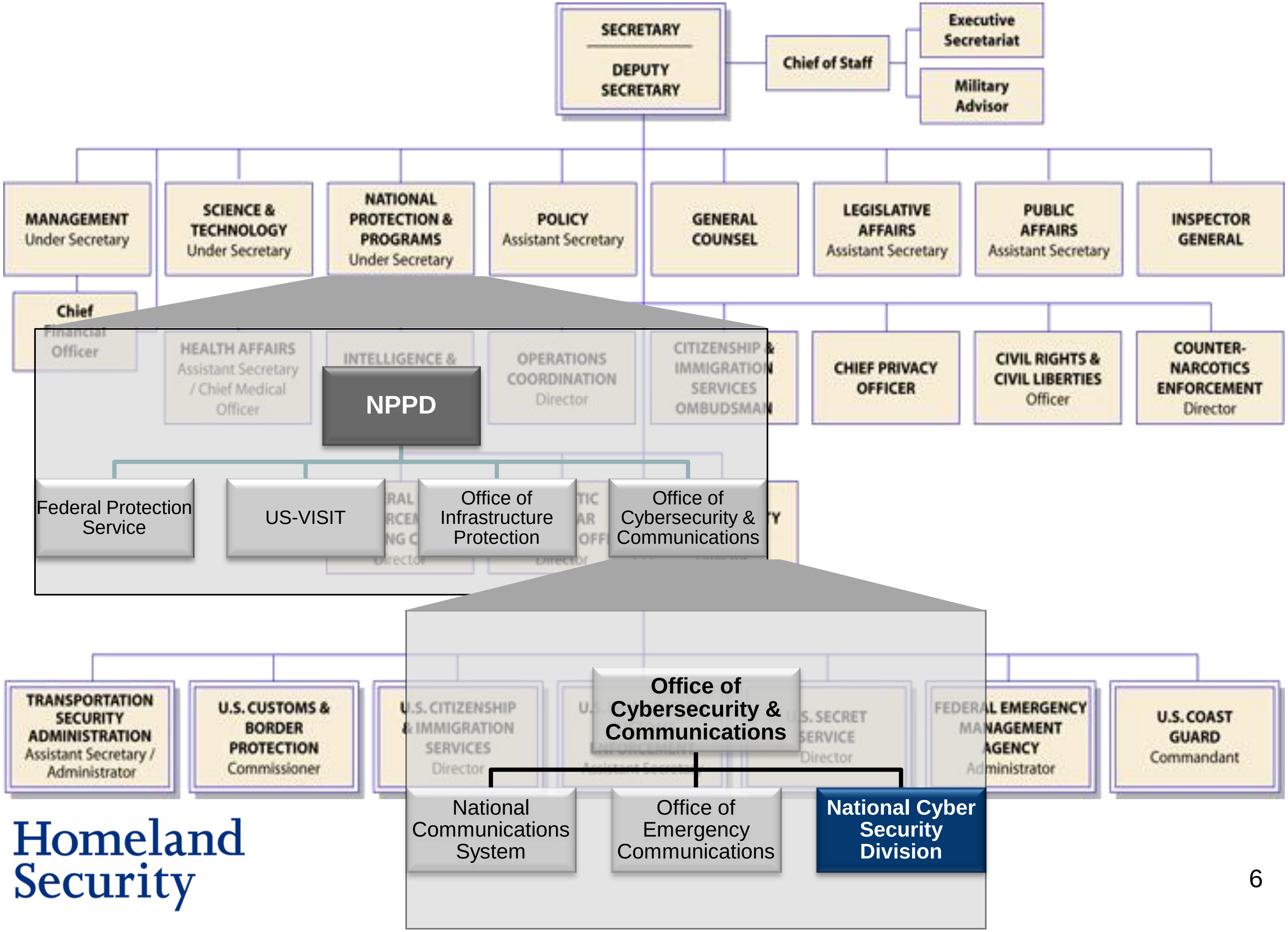
> *"The CARMA methodology has helped ESS work collectively as a large, dispersed group of public partners from across the country. By focusing on cyber risk in manageable phases, we are better able to understand and address our sector's complex, cyber dependencies and interdependencies."*
>
> *- Mark Hogan, Co-Chair, ESS Cyber Security Working Group*

Outcomes

- Conducting CARMA fostered greater cyber collaboration between ESS stakeholders from diverse districts and disciplines
- The finalized list of critical ESS functions and associated cyber infrastructure informs a sector-wide, cyber risk profile which will help determine appropriate incident response
- CARMA will help the sector prioritize risks of concern and determine where to focus their cyber efforts and will link to the ESS cybersecurity roadmap*

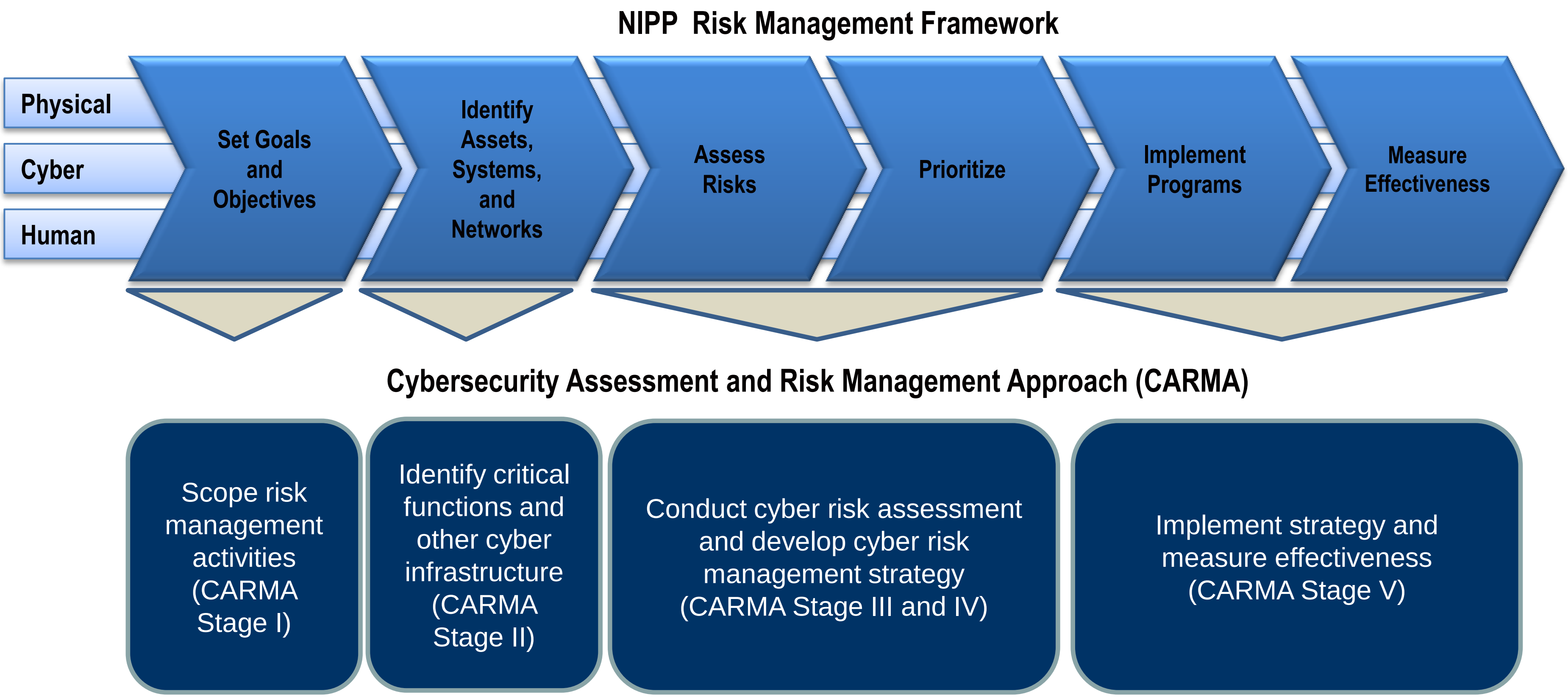
*Roadmap to Secure Voice and Data Systems in the Emergency Services Sector

ESS partnered with DHS's National Cyber Security Division (NCSD), HSPD-7's national focal point for securing cyberspace


SECRETARY
DEPUTY SECRETARY
Chief of Staff
Executive Secretariat
Military Advisor
MANAGEMENT Under Secretary
SCIENCE & TECHNOLOGY Under Secretary
NATIONAL PROTECTION & PROGRAMS Under Secretary
POLICY Assistant Secretary
GENERAL COUNSEL
LEGISLATIVE AFFAIRS Assistant Secretary
PUBLIC AFFAIRS Assistant Secretary
INSPECTOR GENERAL
Chief Financial Officer
HEALTH AFFAIRS Assistant Secretary / Chief Medical Officer
INTELLIGENCE &
OPERATIONS COORDINATION Director
CITIZENSHIP & IMMIGRATION SERVICES OMBUDSMAN
CHIEF PRIVACY OFFICER
CIVIL RIGHTS & CIVIL LIBERTIES Officer
COUNTER-NARCOTICS ENFORCEMENT Director
NPPD
Federal Protection Service
US-VISIT
Office of Infrastructure Protection
Office of Cybersecurity & Communications
TRANSPORTATION SECURITY ADMINISTRATION Assistant Secretary / Administrator
U.S. CUSTOMS & BORDER PROTECTION Commissioner
U.S. CITIZENSHIP & IMMIGRATION SERVICES Director
U.S. SECRET SERVICE Director
FEDERAL EMERGENCY MANAGEMENT AGENCY Administrator
U.S. COAST GUARD Commandant
Office of Cybersecurity & Communications
National Communications System
Office of Emergency Communications
National Cyber Security Division

Homeland Security

Within NCSD, the Critical Infrastructure Protection Cyber Security (CIP CS) Program applies a cyber risk management approach that aligns with traditional CIP efforts



NIPP Risk Management Framework

Physical

Cyber

Human

Set Goals and Objectives

Identify Assets, Systems, and Networks

Assess Risks

Prioritize

Implement Programs

Measure Effectiveness

Cybersecurity Assessment and Risk Management Approach (CARMA)

Scope risk management activities (CARMA Stage I)

Identify critical functions and other cyber infrastructure (CARMA Stage II)

Conduct cyber risk assessment and develop cyber risk management strategy (CARMA Stage III and IV)

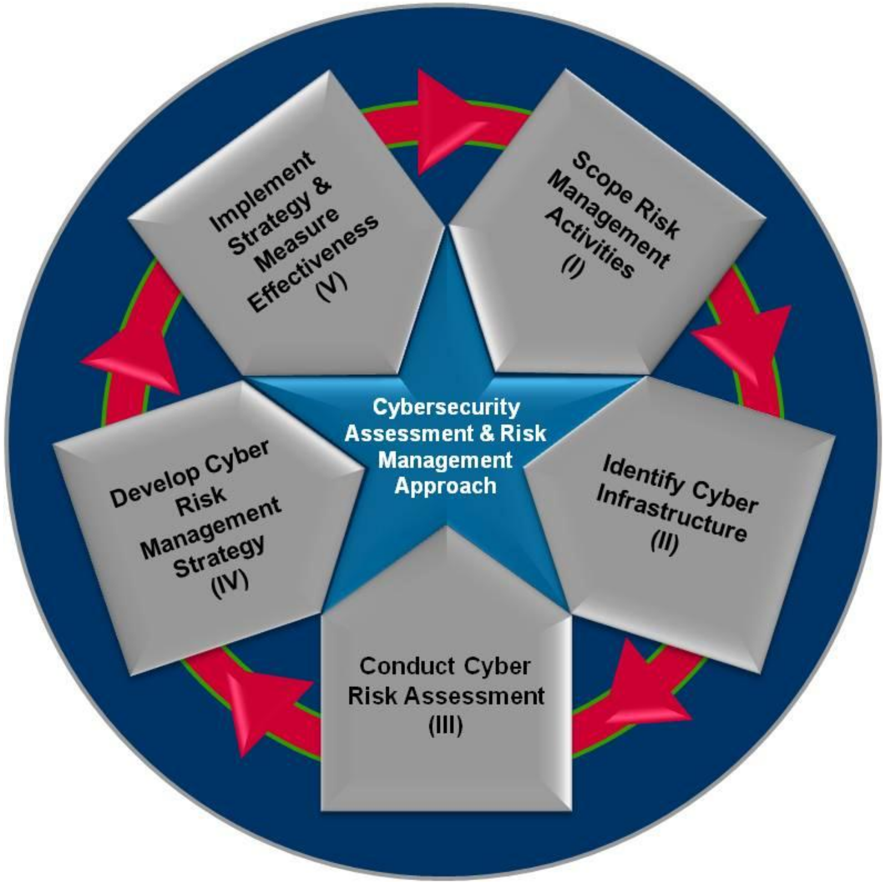
Implement strategy and measure effectiveness (CARMA Stage V)

CARMA provides a strategic view of risk that is best able to address the complex and dynamic nature of cyberspace

The CARMA methodology helped ESS develop and implement a national-level approach to cyber risk management

Cybersecurity Assessment and Risk Management Approach (CARMA)

- Enables partners to effectively identify, assess, and manage national level cyber risks to their infrastructure
- Assists partners in assessing cyber threats, vulnerabilities, and consequences to formulate a cyber risk profile
- Allows partners to identify best practices, programs, subject matter experts, and partners to manage cyber risks to mitigate cyber risk impact to their mission


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

Homeland Security

CARMA results provided the ESS with tangible cyber risk analyses and laid the groundwork for risk management strategies

Risk Priority Matrix

- Summarizes risks to the most basic level
- Prioritizes risks by showing relative likelihood and consequence evaluations

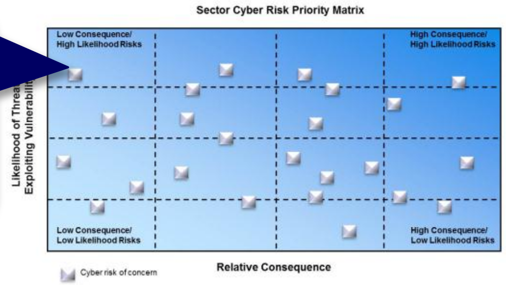
Risk Response Table

- Summarizes strategy for managing identified risks
- Risk response options can be: accept; avoid; transfer; or mitigate.

List of Relevant Protective Programs and R&D

- Captures key initiatives that seek to address risks
- Captures research and development (R&D) efforts that seek to address risks

Cybersecurity Risk Management Snapshot



Activities	Date
Evaluate cross-functional dependencies	October 2011
Evaluate cross-sector interdependencies	December 2011
Update cyber risk assessment methodology	March 2012
Conduct Cyber Risk Assessment 2.0	June 2014

Priority	Risk of Concern	Current Response	Action
0	SCADA Intrusion	Mitigate	Protective Program
1	Access Control System Tampering	Accept	R&D
2	ERP Database Breach	Transfer	Protective Program
3	Hosted Server Breach	Avoid	N/A

Protective Programs

- Control Systems IPS
- Workforce Education Program
- Online Fraud Alerts

Research & Development

- Advanced Control Systems IPS

Metrics

- Have risk responses been identified for key risks?
- For mitigations, is there a plan for development, deployment, and/or implementation?
- Are there measurements or mechanisms for determining if mitigations are reducing risks?

Future Risk Activities Table

- Summarizes areas for future evaluation
- Provides a snapshot of key milestones for risk management activities

Cybersecurity Metrics List/Dashboard

- Articulates the measurements that evaluate risk response implementation
- Can be displayed in list or dashboard format

NOTE: To view an example of what an end product of the assessment can look like, please visit the following link to the IT Sector Baseline Risk Assessment (August 2009): http://www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf. To view an example of what a risk management strategy can look like, please visit the following link to the Domain Name System Risk Management Strategy (June 2011): http://www.dhs.gov/xlibrary/assets/it-sector-risk-management-strategy-domain-name-resolution-services-june2011.pdf
This is not a prescriptive format to follow; just an example. All CARMA evaluations will likely be different and result in unique end products that meet the needs of the stakeholder group conducting the assessment.

Scenario 1: A natural disaster causes the 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

Homeland Security

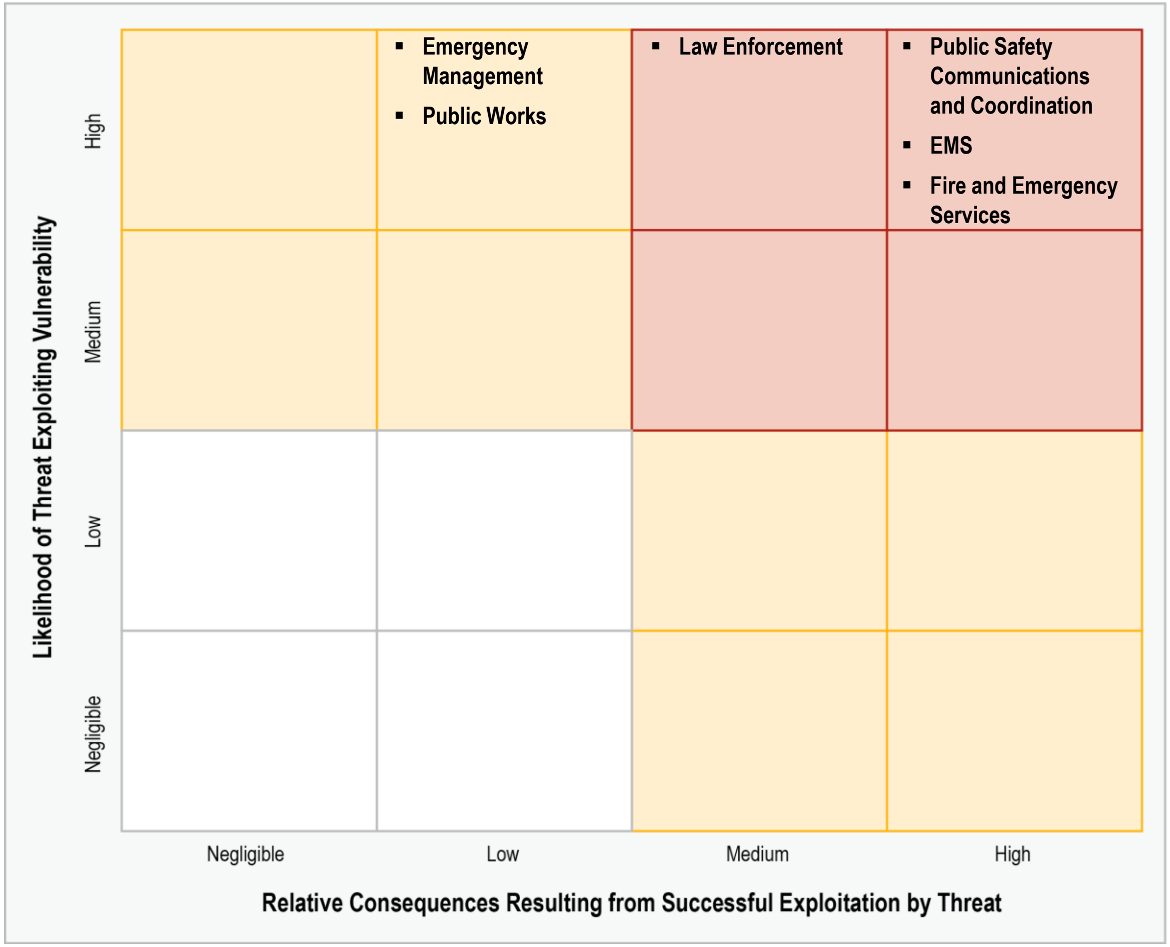
Analysis of Scenario 1 mapped the likelihood and consequence of the risk to each sector function

Relative Risk Profile of Scenario 1:

A natural disaster causes the loss of 9-1-1 capabilities

Natural

Relative Risk Table



Likelihood of Threat Exploiting Vulnerability	Negligible	Low	Medium	High
High		▪ Emergency Management ▪ Public Works	▪ Law Enforcement	▪ Public Safety Communications and Coordination ▪ EMS ▪ Fire and Emergency Services
Medium				
Low				
Negligible				

Relative Consequences Resulting from Successful Exploitation by Threat

Scenario 2: Lack of availability of sector database causes disruption of mission capability

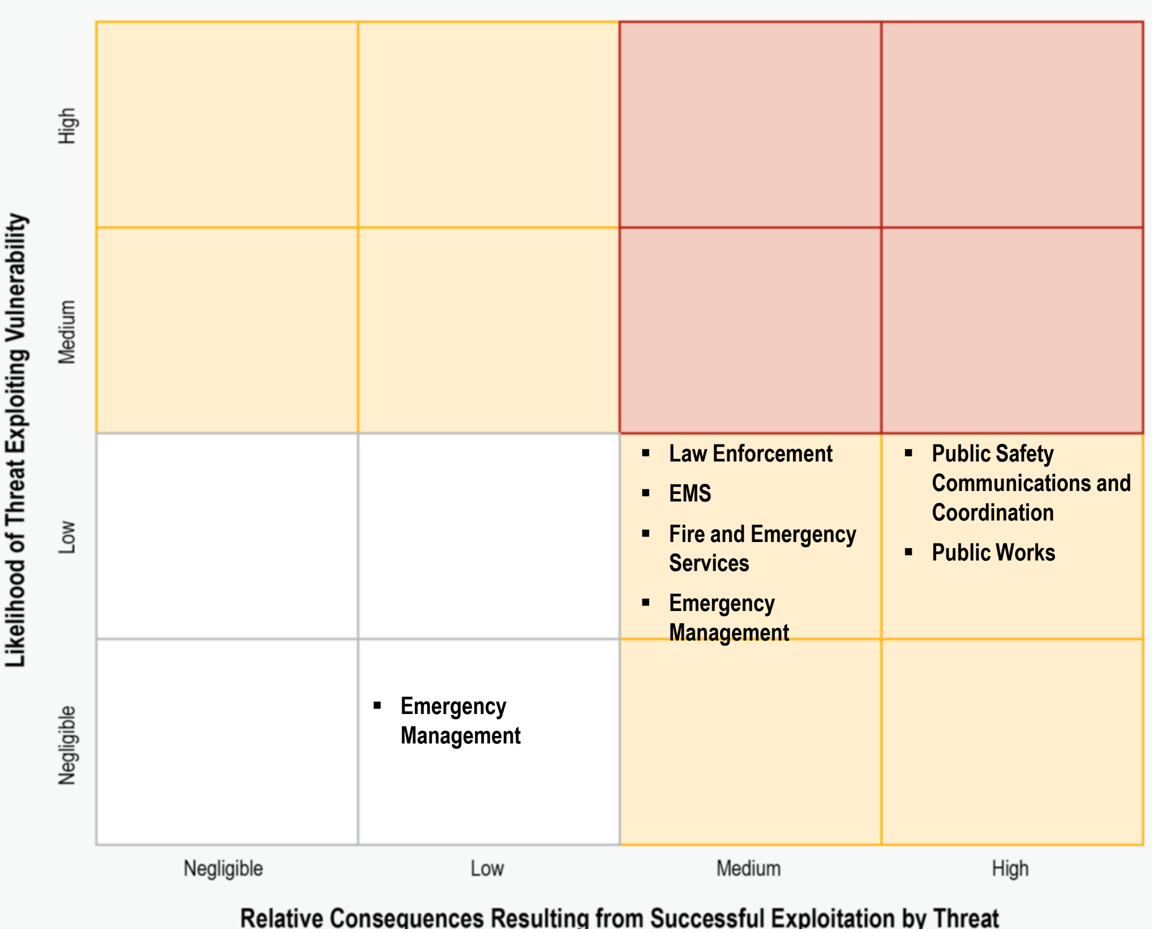
- ESS cyber infrastructure includes databases and their supporting elements
- ESS databases are critical to supporting sector missions and activities
- Should a database be unavailable, there will be disruption to mission capabilities within and across ESS disciplines

Analysis of Scenario 2 mapped the likelihood and consequence of the risk to each sector function

Relative Risk Profile of Scenario 2:

Lack of availability of sector database causes disruption of mission capability

Manmade Unintentional/ Manmade Deliberate

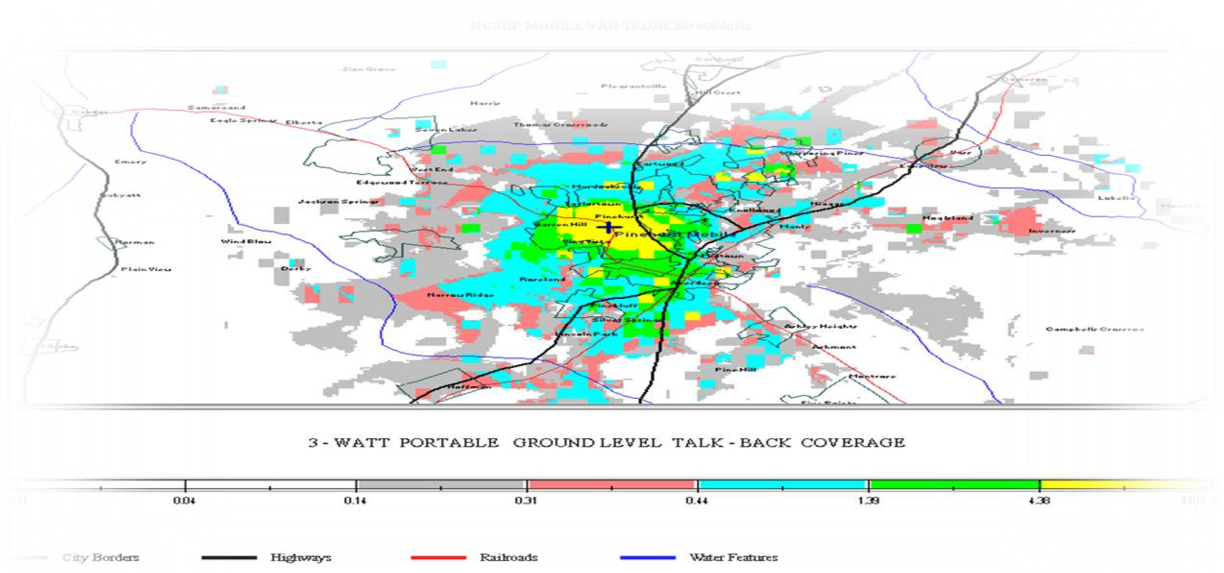


Likelihood of Threat Exploiting Vulnerability	Negligible	Low	Medium	High
High				
Medium				
Low			▪ Law Enforcement ▪ EMS ▪ Fire and Emergency Services ▪ Emergency Management	▪ Public Safety Communications and Coordination ▪ Public Works
Negligible		▪ Emergency Management		

Relative Consequences Resulting from Successful Exploitation by Threat

Scenario 3: Compromised sector database causes corruption or loss of confidentiality of critical information

- 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

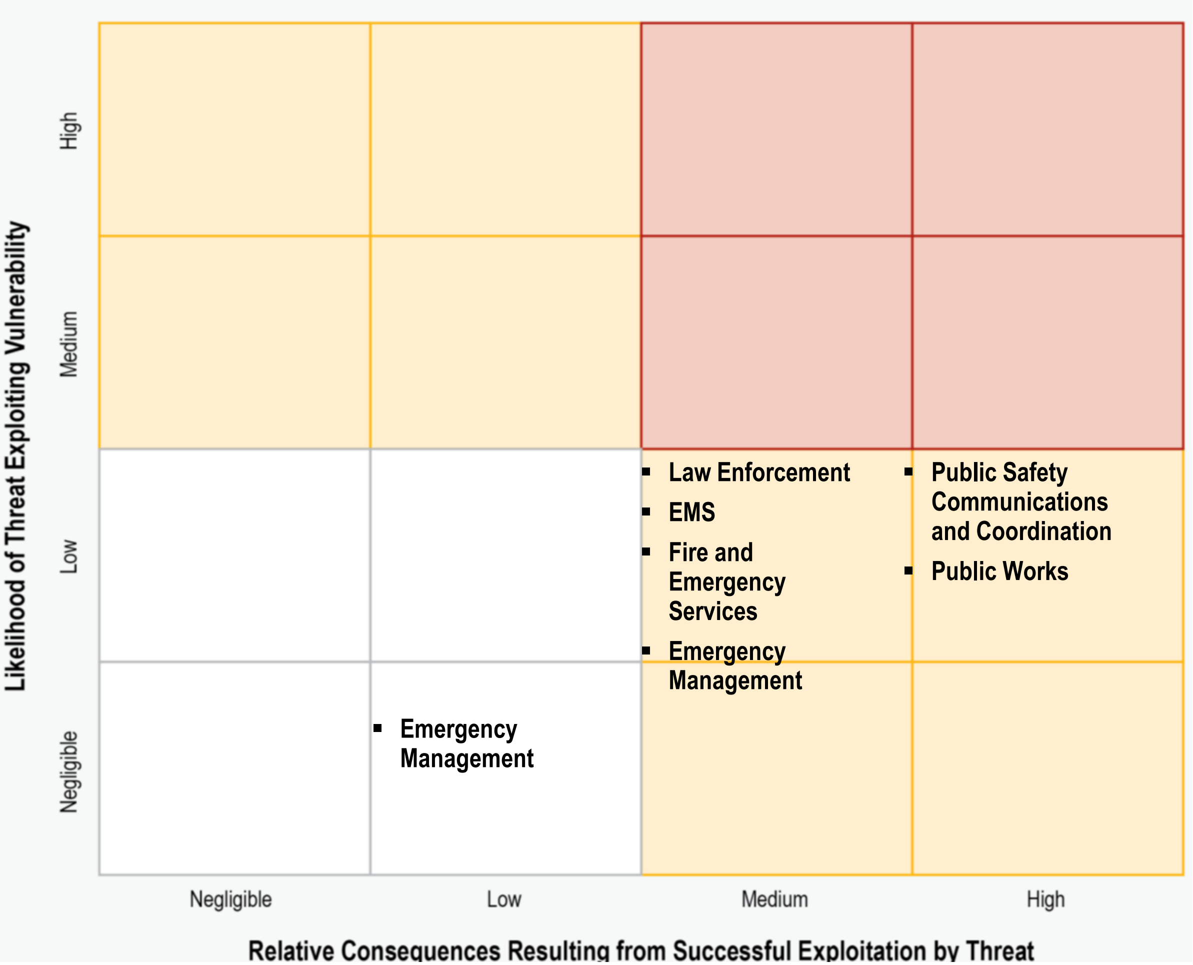


Analysis of Scenario 3 mapped the likelihood and consequence of the risk to each sector function

Relative Risk Profile of Scenario 3:

Compromised sector database causes corruption or loss of confidentiality of critical information

Manmade Unintentional/ Manmade Deliberate



Likelihood of Threat Exploiting Vulnerability	Negligible	Low	Medium	High
High				
Medium				
Low			- Law Enforcement - EMS - Fire and Emergency Services - Emergency Management	- Public Safety Communications and Coordination - Public Works
Negligible		- Emergency Management		

Relative Consequences Resulting from Successful Exploitation by Threat

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 (IPAWS) for major emergencies to regional and local alert and warning systems
- These systems provide alerts for a variety of events and ESS disciplines

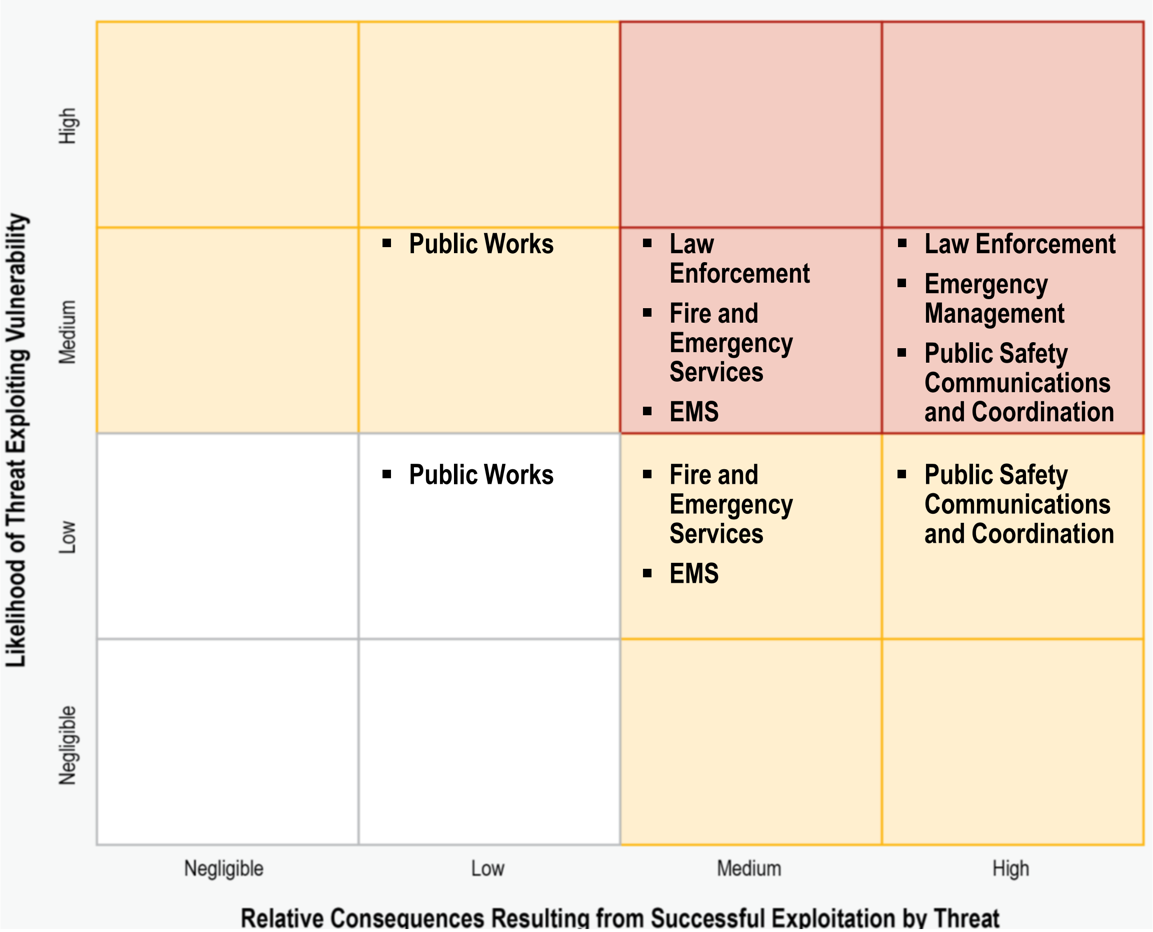
Homeland Security

Analysis of Scenario 4 mapped the likelihood and consequence of the risk to each sector function

Relative Risk Profile of Scenario 4:

Public alerting and warning system disseminates inaccurate information

Manmade Unintentional/ Manmade Deliberate



Likelihood of Threat Exploiting Vulnerability	Negligible	Low	Medium	High
High				
Medium		▪ Public Works	▪ Law Enforcement ▪ Fire and Emergency Services ▪ EMS	▪ Law Enforcement ▪ Emergency Management ▪ Public Safety Communications and Coordination
Low		▪ Public Works	▪ Fire and Emergency Services ▪ EMS	▪ Public Safety Communications and Coordination
Negligible				

Relative Consequences Resulting from Successful Exploitation by Threat

Homeland Security

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 (Natural Disaster)
- 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

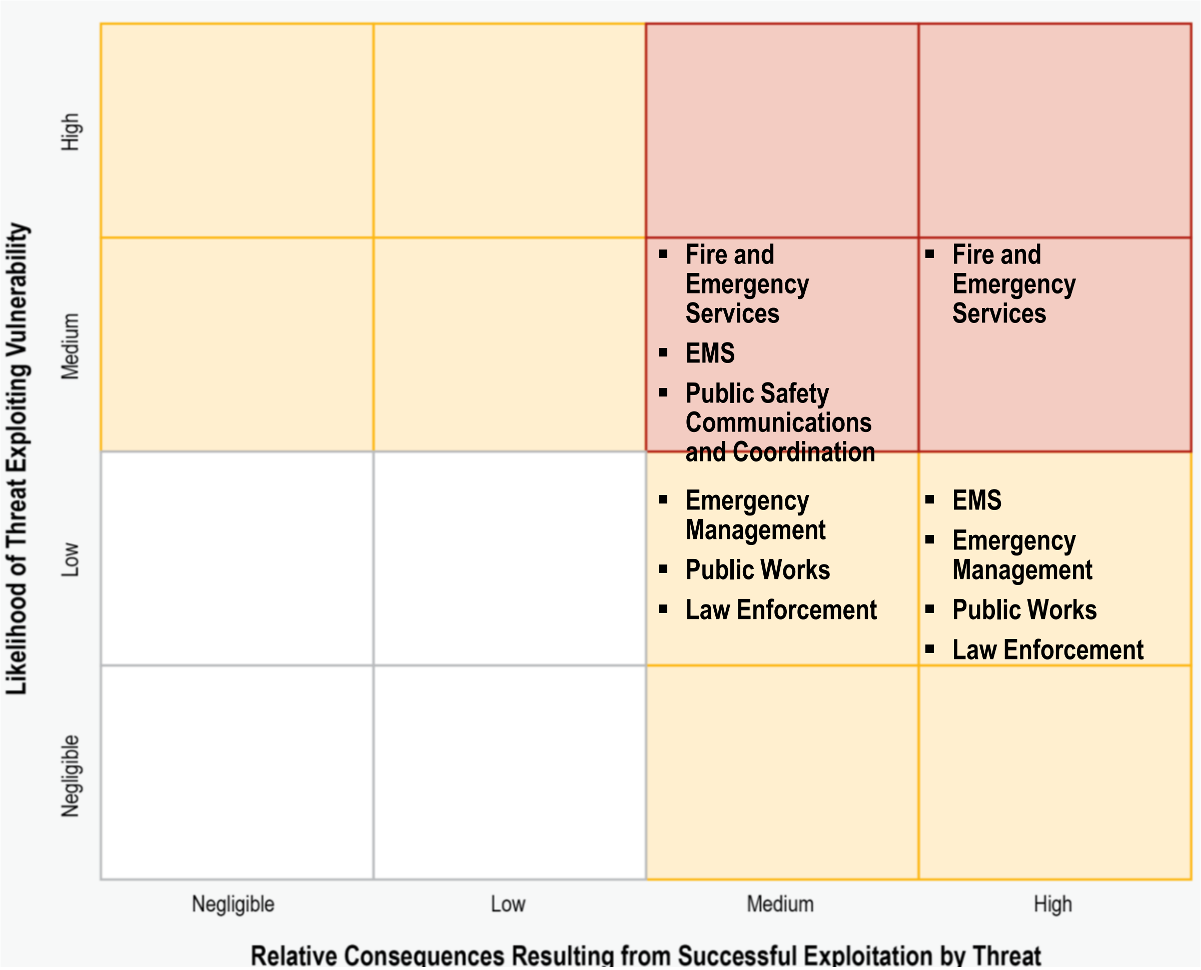
Homeland Security

Analysis of Scenario 5 mapped the likelihood and consequence of the risk to each sector function

Relative Risk Profile of Scenario 5:

Loss of communications lines results in disrupted communications capabilities

Manmade Unintentional/ Manmade Deliberate



Likelihood of Threat Exploiting Vulnerability	Negligible	Low	Medium	High
High				
Medium			▪ Fire and Emergency Services ▪ EMS ▪ Public Safety Communications and Coordination	▪ Fire and Emergency Services
Low			▪ Emergency Management ▪ Public Works ▪ Law Enforcement	▪ EMS ▪ Emergency Management ▪ Public Works ▪ Law Enforcement
Negligible				

Relative Consequences Resulting from Successful Exploitation by Threat

Homeland Security

Scenario 6: Closed-Circuit Television (CCTV) jamming/blocking results in disrupted surveillance capabilities

- 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

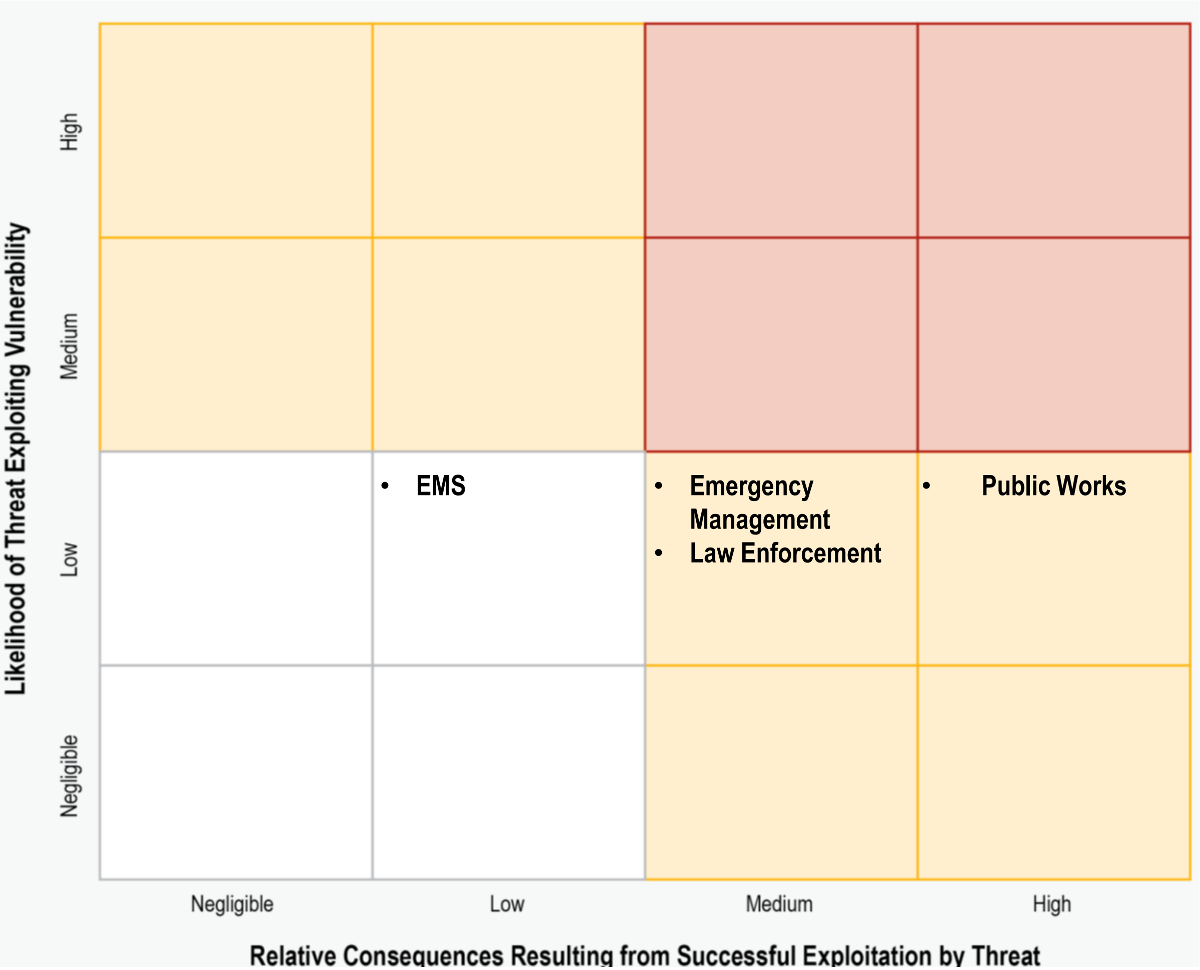
Homeland Security

Analysis of Scenario 6 mapped the likelihood and consequence of the risk to each sector function

Relative Risk Profile of Scenario 6:

Closed-Circuit Television (CCTV) jamming/blocking results in disrupted surveillance capabilities

Manmade Deliberate



Likelihood of Threat Exploiting Vulnerability	Negligible	Low	Medium	High
High				
Medium				
Low		• EMS	• Emergency Management • Law Enforcement	• Public Works
Negligible				

Relative Consequences Resulting from Successful Exploitation by Threat

Homeland Security

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 Public Safety Communications & Coordination/Fusion 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

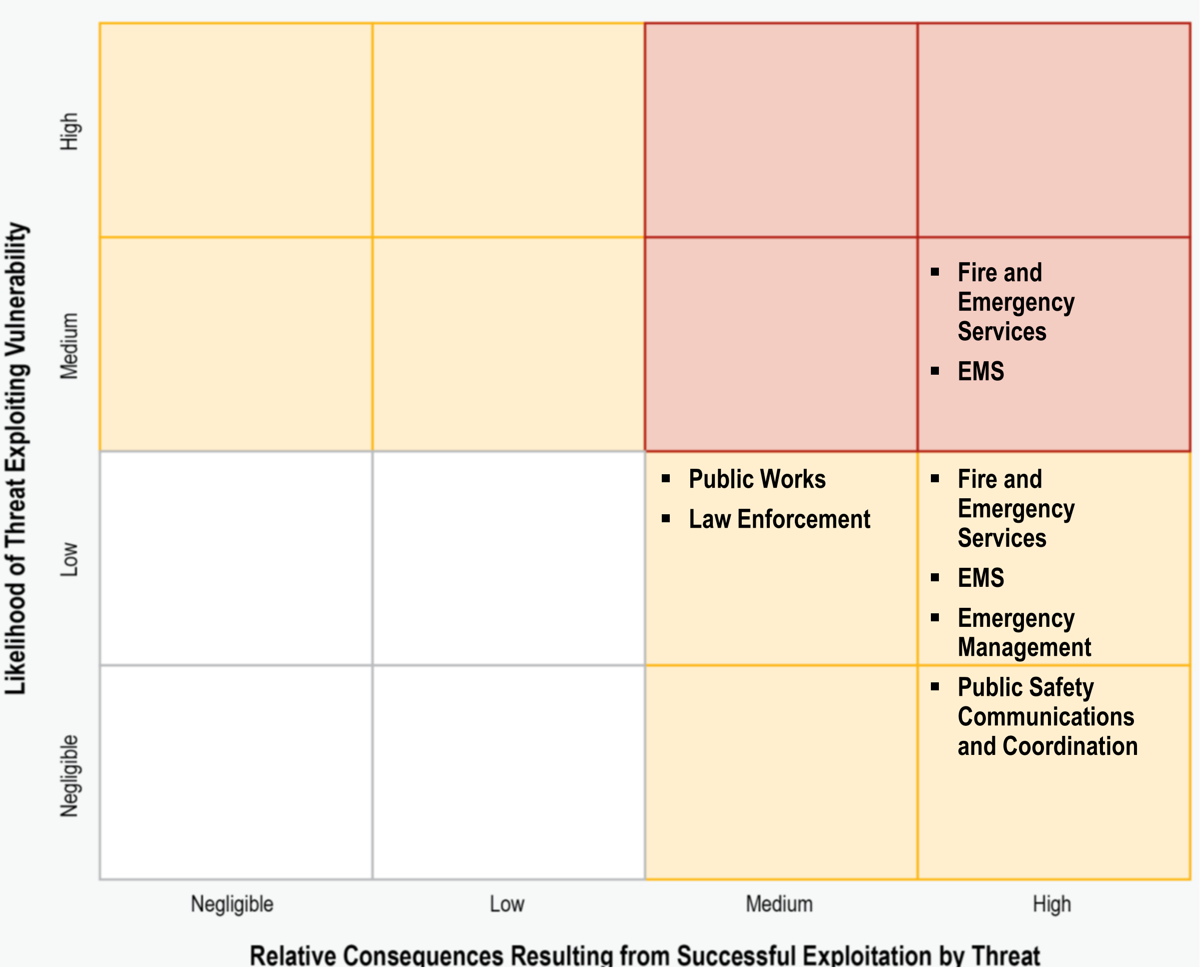
Homeland Security

Analysis of Scenario 7 mapped the likelihood and consequence of the risk to each sector function

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



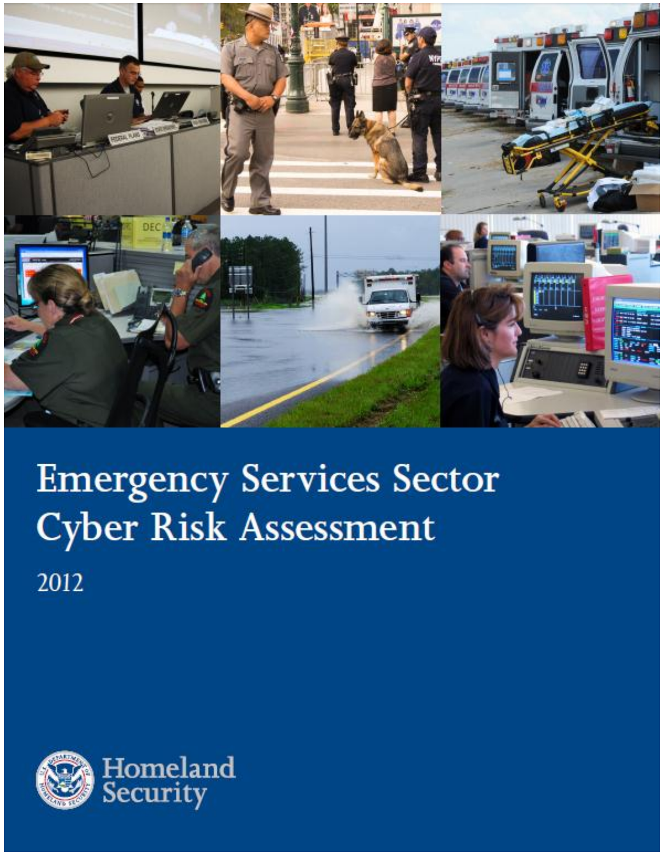
Likelihood of Threat Exploiting Vulnerability

	Negligible	Low	Medium	High
High				
Medium				▪ Fire and Emergency Services ▪ EMS
Low			▪ Public Works ▪ Law Enforcement	▪ Fire and Emergency Services ▪ EMS ▪ Emergency Management
Negligible				▪ Public Safety Communications and Coordination

Relative Consequences Resulting from Successful Exploitation by Threat

The sector is currently in the risk management phase of CARMA, where members decide on responses to the cyber risks

- Sector members are currently deciding which risk response(s) below is most appropriate for each of the cyber risks identified in the ESS-CRA:
  - Avoid the risk
  - Accept the risk and its potential consequences
  - Transfer the risk to another entity, capability, or function
  - Mitigate the risk by using preventative or proscriptive action
- The risk responses and mitigation prioritization will inform resource allocation to respond to threats, vulnerabilities, and/or consequences facing the critical ESS functions
- Results from the sessions will be published in the *Roadmap to Secure Voice and Data Systems in the ESS*



Emergency Services Sector Cyber Risk Assessment

2012

Homeland Security

CARMA allowed ESS to evaluate consequences of cyber incidents and identify areas for future emphasis

Connect and frame existing sector cybersecurity activities

- CARMA results can provide a strategic framework for facility- or asset-based cybersecurity plans, assessments, and other activities
- CARMA highlights shared risks across sector infrastructure to identify areas for increased attention

Help address the entire risk equation: threats, vulnerabilities, and consequences

- Scenarios can identify and/or facilitate future areas for stakeholder training
- While CARMA helps sector members to fill out threat and vulnerability information affecting their infrastructure, CARMA also has a unique focus on conducting consequence evaluations of cyber threats, not present in most assessments

Identify, assess, and manage cyber risk

- The sector can acquire a greater understanding of strategic risks identified through the risk assessment process and corresponding risk responses
- CARMA helps provide a strategic framework for understanding how threat scenarios/incidents impact sector critical functions

Emerging issues in the ESS will influence the scope of future updates to the risk assessment

Next Generation 9-1-1

- Next Generation 9-1-1 will permit new access points for voice, data, and video on public safety telephone networks
- This could introduce the potential for viruses and other threats

Cloud Computing

- Cloud computing is a tempting new opportunity for IT system managers to gain greater computing capabilities and more optimal use of networks
- However, cyber threats associated with this capability as it impacts public safety networks and services have not yet been determined

Nationwide Public Safety Broadband Network (NPSBN)

- The NPSBN promises voice, data, and video on a network exclusively for Federal, State, local, and tribal public safety providers
- With interfaces to commercial networks, the NPSBN creates openings that we have never faced using our private land mobile radio and computer aided dispatch networks

For more information, please contact:

Jason Gates
U.S. Department of Homeland Security
National Cyber Security Division
Jason.Gates@dhs.gov

Sabrina Hammouda
U.S. Department of Homeland Security
Emergency Services Sector Specific Agency
ESSTeam@hq.dhs.gov

Mark Hogan
City of Tulsa
Chair, Emergency Services Sector Cyber Working Group
MHogan@cityoftulsa.org

U.S. DEPARTMENT OF HOMELAND SECURITY

Homeland
Security