March 10, 2021

COMMUNICATIONS SECURITY, RELIABILITY, AND INTEROPERABILITY
COUNCIL VII

REPORT MEASURING RISK MAGNITUDE AND REMEDIATION COSTS IN 9-1-1 AND NEXT GENERATION 9-1-1 (NG911) NETWORKS

Working Group 4: 911 Security Vulnerabilities during the IP Transition

Table of Contents

1 Results in Brief

1.1 Executive Summary

The Federal Communications Commission (FCC) specifically directed CSRIC VII to study and produce a *Report on Security Risks and Best Practices for Mitigation in 9-1-1 in Legacy, Transitional, and NG9-1-1 Implementations,* focusing on measuring the risk magnitude and remediation costs within those networks. This document, *CSRIC VII Report Measuring Risk Magnitude and Remediation Costs in 9-1-1 and NG9-1-1 Networks,* provides the requested information.

Next Generation 9-1-1 (NG9-1-1) has greater scalability and flexibility than the current 9-1-1 environment. This advanced technology is far more robust and has a greater potential to increase public and first responder safety through interconnectivity and interoperability than the current 9-1-1 environment. IP networks facilitate NG9-1-1 architectures that enable new response capabilities, while also creating potential opportunities for cyber-attacks that can disrupt Public Safety Answering Point/Emergency Communications Center (PSAPs/ECCs) operations. However, the transition from legacy 9-1-1 to the NG9-1-1 networks offers its own set of security risks. As described by the Commission's charge to CSRIC VII, "[t]he transition from legacy to IP-based networks, may result in hybrid system settings that commingle legacy and IP network elements. While in this hybrid state, the 9-1-1 systems operate at higher risk."

This Report complements prior reports: *CSRIC VII Report on the Current State of Interoperability in the Nation's 911 Systems* (Report 1) and *CSRIC VII Report on Security Risks and Best Practices for Mitigation in 9-1-1 in Legacy, Transitional, and NG9-1-1 Implementations* (Report 2); that focus on findings and recommendations related to measuring the risk magnitude of cyber threats and the associated estimated remediation expense associated with threat surfaces and potential attack vectors related to ECCs. Historically, in prior reports released by CSRIC VII, one can find information regarding the various transitional phases involved in migrating from legacy 9-1-1 networks to fully operational next generation IP networks supporting NG9-1-1 functions and processes. As discussed in Report 2, CSRIC VII determined that several of the transitional phases did not materially impact the nature of cyber-security during the transition, and CSRIC VII consolidated NG9-1-1 transitional stages into only three. This report remains consistent with those architectural recommendations focusing on the Legacy, Transitional, and End State architectures, as recommended in Report 2.

This report examines the nature of those attack surfaces and vectors, along with potential remediation strategies to mitigate their impact and associated costs. As in Report 2, the analysis and recommendations in this report are based on Council member experience, an exploration of the available growing body of literature and documented experience in the industry today. This report identifies extensive findings that drive a wide range of measures for mitigating the effects of cyber-risks. Section 5.2.1 below describes numerous industry-tested mitigation strategies that can be used by PSAPs/ECCs. The report also identifies the potential cost and level of effort for these measures, providing a roadmap for organizations of different sizes and capabilities to

improve their cybersecurity posture regardless of the level of a given organization's cybersecurity maturity. The report's findings consider "soft" measures, like cybersecurity hygiene training and identifying a single individual responsible for cybersecurity, as well as technical measures, like network segmentation and active network monitoring.

In this report, CSRIC VII expanded the work completed in Report 2, by reviewing existing industry Best Practices related to cybersecurity practices and adding 37 new Best Practices, Appendix A - Proposed Best Practices, that will assist not only the private sector 9-1-1 industry, but also the Public Safety community involved in deployment of 9-1-1 networks. The new Best Practice recommendations range from training of personnel in cybersecurity practices, to applications of information spoofing mitigation.

A major goal of this report was related to quantifying cyber risks and determining cost to mitigate those risks. The need to manage cyber risk is more pressing than ever. According to the World Economic Forum's *The Global Risks Report 2018*[1], cyberattacks rank No. 3 among the top ten risks for businesses in terms of *likelihood*, outranked only by extreme weather events and natural disasters. In terms of *impact*, cyberattacks didn't even make the list in 2017—but today cyberattacks is listed at No. 6. In the World Economic Forum's, *The Global Risks Report 2021,*[2] cybersecurity failure ranks No. 4 among the top ten "Clear and Present Dangers" for businesses.

As cyber risk grows, so does the need to quantify it. Without quantifying risk, how can an organization calculate how much cyber insurance it needs? Or how does an organization prioritize investments in security controls based on where it sees the most risk? Or how does an organization calculate the return on those investments? This reprt takes readers through the benefits of quantifying cyber risks, assists organizations in a methodology for quantifying cyber risks, and makes strong recommendations on 9-1-1 funding priorities related to planning and implementation of critical cybersecurity investments. This report also recommends the FCC expand its annual data collection on the use of 9-1-1 funds to include more robust information on the inclusion of cybersecurity planning and mitigation expenditures and that cybersecurity investments should be an explicit valid use of 9-1-1 funds. CSRIC VII also strongly supports the FCC's efforts to stop 9-1-1 fee diversion and recognizes such reckless use of public funds not only negatively impacts the deployment of critical 9-1-1 services, it also harms 9-1-1 cybersecurity planning.

Section 5.3 includes extensive recommendations that cover the critical elements of planning for cybersecurity risks and provides valuable insight on mitigation techniques. Readers will gain insight into cyber response plans and the value those plans play in minimizing risks to 9-1-1. This report describes a variety of mitigation strategies that should be deployed to prevent, and, if necessary, respond to cyber threats. Such strategies include, but are not limited to:

- Cyber Security Best Practices (see Appendix A - Proposed Best Practices, and Best Practices | Federal Communications Commission (fcc.gov))

[1] World Economic Forum (WEF), The Global Risks Report 2018, 13th Edition, p. 3
[2] See World Economic Forum (WEF), The Global Risks Report 2021, 16th Edition, p. 11. Retrieved 3 February 2021 at https://www.weforum.org/reports/the-global-risks-report-2021.

- Identification of a Chief Information Security Officer (CISO) for every organization involved in this process
- Continuous Cyber Monitoring
- Vulnerability Assessments
- Backups on different forms of media storage
- A well-documented, written cyber response plan
- Affirmative cyber insurance coverage
- Network and system cyber security features
- Staff well trained in identifying and remediating cyber vulnerabilities and practicing necessary cyber-hygiene

CSRIC VII recommendations also include advice on future roles the FCC can play in this process that will aid in encouraging the industry to plan and implement cyber response and mitigation plans. The report also recommends the Commission seek CSRIC support to continue its research on:

- Over-the-top network solutions, such as Text To 9-1-1 (including examination and consideration of teletypewriter (TTY) architectures),
- Cyber vulnerabilities and cyber threat exposure related to delivery of supplemental data to PSAPs / ECCs and the use of handset-based applications,
- IoT as a cyberattack target,
- Smart Cities,
- 5G,
- How to deal with encrypted data before it reaches the PSAP/ECC; and
- Other cybersecurity topics as they become known.

In summary, CSRIC VII is honored to publish a report that meets the unique needs of 9-1-1 networks, as they transition to Next Generation 9-1-1 architectures. This report can serve as the foundation for educating the industry on cyber risks, the need for robust cyber response plans and will assist the FCC with future initiatives related to cybersecurity and 9-1-1.

2 Introduction

In early December 2020, the Cybersecurity and Infrastructure Security Agency (CISA) issued an emergency directive focused on the compromise of Solarwinds Orion Network Management products.[3] This Emergency Directive called on all federal civilian agencies to review their networks for indicators of compromise and disconnect or power down SolarWinds Orion products immediately. SolarWinds supply chain software is widely used by federal, state, and local governments, as well as critical infrastructure entities and other private sector organizations, including the telecommunications industry.[4] A new, similar attack was identified in early February.[5] As of the date of this report, the total impact of this series of compromises continues to be investigated.

The above incident emphasizes that cyber risk is becoming more sophisticated every day. Preventing and being prepared for that risk is critical to public services that are, by nature, highly exposed to that risk. That is true of public safety communications, and specifically 9-1-1 services that support the public's access to emergency response.

The 9-1-1 Industry is currently in the process of migrating NG9-1-1. NG9-1-1 is based on the use of Internet Protocol (IP) networks that enable interconnection and interoperability on a wide range of public and private networks, and, in the process dramatically improve emergency service to the public. Unfortunately, this increased level of service brings with it increase risk to the public safety system, for, as the US Department of Homeland Security (DHS) points out, ". . . cyber risks do present a new level of exposure that PSAPs must understand and actively manage as a part of a comprehensive risk management program."[6]

As CSRIC VII has previously noted, 9-1-1 systems are highly interconnected, and interoperability between call-taking and call processing components is critical. Legacy, transitioning, and fully NG9-1-1-capable systems capture and exchange potentially large amounts of data and transferring such data between 9-1-1 systems potentially requires external data connections. The presence of such connections expands the cyber-attack surface of the network.

The transition from legacy 9-1-1 to NG9-1-1 networks offers its own set of security risks. As described by the FCC's charge to CSRIC VII, "[t]he transition from legacy to IP-based networks, may result in hybrid system settings that commingle legacy and IP network elements. While in this hybrid state, the 911 systems operate at higher risk."[7]

---

[3] CISA Issues Emergency Directive to Mitigate the Compromise of Solarwinds Orion Network Management Products | CISA, December 13, 2020, see: https://www.cisa.gov/news/2020/12/13/cisa-issues-emergency-directive-mitigate-compromise-solarwinds-orion-network. SolarWinds Inc. is an American company that develops software for businesses to help manage their networks, systems, and information technology infrastructure.
[4] See: Supply Chain Compromise | CISA, see: https://www.cisa.gov/supply-chain-compromise
[5] See https://www.reuters.com/article/us-cyber-solarwinds-china-idUSKBN2A22K8.
[6] US Department of Homeland Security, Office of Emergency Communications, "Cyber Risks to Next Generation 911, see:
https://www.911.gov/pdf/OEC_NG9-1-1_Cybersecurity_Primer_041216_508_compliant.pdf
[7] See: https://www.fcc.gov/files/csric7wgdescriptionsdocx

With this in mind, the FCC directed CSRIC VII, via Working Group 4 (WG4), to survey the current state of interoperability for the nation's 9-1-1 systems, including for legacy 9-1-1 networks, transitional 9-1-1 networks, and NG9-1-1. The FCC further directed CSRIC VII WG4 to identify security risks in legacy 9-1-1 networks, transitional 9-1-1 networks, and NG9-1-1 networks and recommend best practices to mitigate risks in these three areas. In addition, CSRIC VII WG4 will place the vulnerabilities on a scale that accounts for both risk level and remediation expense. This work is encompassed in three milestone reports:

1. CSRIC VII Report on Current 9-1-1 Systems Interoperability (March 2020)
2. CSRIC VII Report on Security Risks and Best Practices for Mitigation in 9-1-1 in Legacy, Transitional, and NG9-1-1 Implementations (September 2020)
3. CSRIC VII Report Measuring Risk Magnitude and Remediation Costs in 9-1-1 and NG9-1-1– Networks (March 2021)

This is the final of the three Reports, dealing specifically with the measurement of "Risk Magnitude and Remediation Costs in 9-1-1 and NG9-1-1-Networks," and placing those vulnerabilities on a scale that accounts for both risk level and remediation expense. This report complements the second report published by CSRIC VII titled, *CSRIC Report on Security Risks and Best Practices for Mitigation in 9-1-1 in Legacy, Transitional, and NG9-1-1 Implementations*, and focuses on the threat surface and potential attack vectors related to emergency communications centers.

2.1 CSRIC VII Structure

CSRIC VII was established at the direction of the Chairman of the Federal Communications Commission in accordance with the provisions of the Federal Advisory Committee Act, 5 U.S.C. App. 2. The purpose of CSRIC VII is to provide recommendations regarding ways the FCC can strive for security, reliability, and interoperability of the nation's communications systems. CSRIC VII's recommendations will focus on a range of public safety and homeland security-related communications matters. The FCC created informal subcommittees under CSRIC VII, known as working groups, to address specific tasks. These working groups must report their activities and recommendations to the Council as a whole, and the Council may only report these recommendations, as modified or ratified, as a whole, to the Chairman of the FCC.

Communications Security, Reliability, and Interoperability Council (CSRIC) VII					
CSRIC VII Working Groups					
Working Group 1: Alert Originator Standard Operating Procedures & Duplicate NWS Alert	Working Group 2: Managing Security Risk in the Transition to 5G	Working Group 3: Managing Security Risk in Emerging 5G Implementations	Working Group 4: 911 Security Vulnerabilities during the IP Transition	Working Group 5: Improving Broadcast Resiliency	Working Group 6: SIP Security Vulnerabilities

Chair: Craig Fugate, APTS/ CoChairs: Michelle Mainelli, NWS Terri Brooks, T-Mobile	Chair: Kathy Whitbeck, Nsight	Chair: Farrokh Khatibi, Qualcomm	Chair: Mary Boyd, West Safety Services	Chair: Pat Roberts, Florida Association of Broadcasters	Chair: Danny McPherson, Verisign
FCC Liaisons: James Wiley,/ David Munson	FCC Liaison: Kurian Jacob	FCC Liaison: Steven Carpenter	FCC Liaison: Rasoul Safavian	FCC Liaison: Robert "Beau" Finley	FCC Liaison: Ahmed Lahjouji

Table 1 - Working Group Structure

2.2 *Working Group 4 Team Members*

Name	Company
Mary A. Boyd, Chair	Intrado Life & Safety
Brandon Abley	NENA: The 9-1-1 Association
Daryl Branson	Colorado Public Utilities Commission
Roger Marshall	Comtech
Gerald "Jay" English	Association of Public Safety Communications Officials (APCO)
Laurie Flaherty	U.S. Department of Transportation
Jay Gerstner (Alternate: Robert Dianda)	Charter Communications
James (Jim) Goerke (Alternate: Richard Muscat)	Texas 9-1-1 Alliance
Stacy Hartman	Lumen
William (Mike) Hooker (Alternate: Jeanna Green)	T-Mobile USA
Gerald (Jerry) Jaskulski	Cybersecurity and Infrastructure Security Agency (CISA)
William (Andy) Leneweaver	Washington State 911 Coordination Office
Tim Lorello (Alternate: Tom Breen)[8]	SecuLore Solutions
Krisztina Pusok	American Consumer Institute
Theresa Reese	Ericsson
Charlie Sasser	National Association of State Technology Directors (NASTD)
Andre Savage	Cox Communications
Dorothy Spears-Dean	National Association of State 911 Administrators (NASNA)
Leslie Sticht	State of Minnesota
Mark Titus	AT&T
Brian Trosper (Alternate: Bill Mertka)	Verizon
Jeff Wittek	Motorola Solutions
Jackie Wohlgemuth	ATIS
FCC Liaison, Rasoul Safavian	

Table 2 - List of Working Group Members

[8] Tom Breen represented Comtech on the WG from 7/2019 through 7/2020.

3 Objective, Scope, and Methodology

3.1 Objectives

CSRIC VII, Working Group 4, Report 3:
Report Measuring Risk Magnitude and Remediation Costs in 911 and NG911 Networks

The previous CSRIC VII report (Report 2) focused on the cybersecurity[9] risks inherent in any IP based network or system, with particular focus on the threat surface and potential attack vectors as they relate to ECCs. This third and final report by CSRIC VII WG4 is focused on identifying the level of risks and the estimated remediation costs necessary to ensure effective operation of the ECCs in the face of any experienced cyberattacks.

With the benefits of IP-enabled NG9-1-1 comes the inherent need to defend the network/system(s) against cyberattacks that could impact the ability of a PSAP to serve their citizenry effectively. These types of cyberattacks have already happened in jurisdictions across the USA. See Section [5.1.1]. Hence the value of this type of analysis of the risk magnitude and remediation costs that public safety and the associated network vendor community will encounter when dealing with cyber breaches and attacks.

This final report of CSRIC VII provides guidance on the following subjects in order to achieve the primary objective stated above:

1. Providing analysis that clearly stablishes the need for adequate cyberattack monitoring and defense solutions in PSAPs/ECCs in the wake of the transition to NG9-1-1.
2. Identifying cost estimates associated with viable cyberattack monitoring and defense solutions.
3. Identifying cost estimates associated with implementing the recommended Best Practices related to achieving viable cyberattack monitoring and defense solutions.
4. Identifying which Best Practices could be implemented to improve cybersecurity posture for PSAPs/ECCs in a relatively short time frame and at a moderate and manageable cost.

3.2 Scope

In addition to the review of hybrid 911 system architectures that commingle legacy and IP network elements, the Working Group will:

- ❑ Identify and place vulnerabilities on a scale that accounts for risk level;
- ❑ Study risk levels and develop remediation expense;
- ❑ Review Best Practices and make recommendations to reduce vulnerabilities;

[9] For the purposes of this document, the scope of "cybersecurity" is the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation, as well as procedures for detecting, responding to and recovering from incidents when such protections fail.
https://niccs.us-cert.gov/about-niccs/cybersecurity-glossary

- ❑ Identify any economic disadvantages or risks;
- ❑ Identify any barriers to implementing mitigation measures; and
- ❑ Publish a report measuring risk magnitude and remediation costs in 9-1-1 and NG9-1-1 systems.

3.3 Methodology

As described above, CSRIC VII was responsible for three reports focused on 9-1-1 security vulnerabilities during the community's transition to an IP based service platform. The first report examined available data and information that would support report observations on the state of interoperability among 9-1-1 systems transitioning to the NG 9-1-1.[10] That included a review of current published data on such matters along with contributions from the 9-1-1 community provided by APCO, NASNA, and the National 9-1-1 Program. CSRIC VII looked to the "maturity states" adopted by the FCC's earlier TFOPA reports to guide its report formulation, based on the assumption that state of national NG9-1-1 interoperability was largely a function of the attainment of those states by the various jurisdictional entities involved in providing 9-1-1 service across the nation.[11]

In Report 2, dealing with *Security Risks and Best Practices for Mitigation in 9-1-1 in Legacy, Transitional, and NG9-1-1 Implementations*, CSRIC VII determined that three separate intermediate states did not materially impact the nature of cybersecurity during the process of transitioning to end-state NG9-1-1 and combined those states into one "transition" and one "end state," for the purposes of the report, resulting in the three 9-1-1 service states of "legacy, transition and end-state."[12] CSRIC VII assumed that cybersecurity requirements for each state would vary to some degree and based the report on that assumption. Within the context of these states, CSRIC VII examined the various attack "surfaces and vectors" employed by today's "bad actors" based upon the experience of Council members, and relevant third-party resources, including but not limited to the above TFOPA reports.

This report on the measurement of *Risk Magnitude and Remediation Costs in 9-1-1 and NG9-1-1– Networks* builds on the previous two reports by examining the nature of those attacks, along with attack mitigation and remediation strategies and the associated cost. As in Report 2, this was based on Council member experience and an exploration of available growing literature and documented experience in the industry today.

---

[10] CSRIC VII Report on the Current State of Interoperability in the Nation's 911 Systems (March 2020). See: https://www.fcc.gov/file/18394/download

[11] Task Force on Optimal Public Safety Answering Point Architecture (TFOPA), Working Group 2, "Phase II Supplemental Report: NG9-1-1 Readiness Scorecard," p13, December 2, 2016, see: https://transition.fcc.gov/pshs/911/TFOPA/TFOPA_WG2_Supplemental_Report-120216.pdf . The TFOPA activity defined states of transition ranging from today's legacy state, through foundational, transitional, and intermediate states, culminating in the jurisdictional and nation-wide "end states" of NG9-1-1 service.

[12] CSRIC VII Report on Recommendations and Best Practices for Mitigation in 911 Legacy, Transitional and NG9-1-1 (September 2020). See: csric7_report_secuirtyrisk-bestpracticesmitigation-legacytransitionalNG9-1-1.pdf | Federal Communications Commission (fcc.gov)

In addition, this report addresses Best Practices related to the mitigation of cybersecurity risks. In reviewing existing Best Practices, it was determined that, while a number of them addressed cybersecurity considerations in legacy, transitional, and/or end-state NG9-1-1 environments, there were some that would benefit from further clarification with respect to the functionality supported, the roles to which they applied, or their applicability to emergency services. CSRIC VII also proposes the deletion of some existing Best Practices due to redundancy. In addition, based on an analysis of the use cases and cybersecurity controls provided in Report 2, several new Best Practices were identified. The new Best Practices address topics such as the need for the training of Public Safety staff in cybersecurity practices and the specification of operational procedures to prevent or more easily detect intrusion or other attacks, as well as improvements in traffic monitoring, network resiliency, data protection, and cybersecurity attack response. In addition, the new Best Practices address the application of information spoofing mitigation mechanisms to emergency, callback, and administrative calls as part of an overall security strategy to mitigate Telephony Denial of Service (TDoS), swatting or other types of attacks.

4 Background

9-1-1 and public safety have been a very high priority for the FCC since the early 1990's.

During the prior CSRIC VI (2016 – 2018), Working Group 1 (WG1) focused on NG9-1-1 and the nation's transition from legacy 9-1-1 circuit switched network call handling platforms to NG9-1-1 IP-based Emergency Services IP networks (ESInets) and core services. Its report stated, "The migration presents the opportunity to assess the reliability and resiliency of the networks and FEs supporting the transition."

As CSRIC VI completed its work on minimizing the risk of outages during the transition from legacy 9-1-1 to NG9-1-1, it became very apparent that cybersecurity needed to be considered as a potential risk, and this fact was documented in the final report. As that report states: "the public safety community must continually identify risks and address evolving physical and cybersecurity requirements."[13] CSRIC VI noted that the rapid rate of technology advancement continued to outpace the public safety community's ability to stay ahead of the threats.

Following the advice of CSRIC VI recommendations, the Commission directed CSRIC VII to:

- Survey the current state of interoperability for the nation's 9-1-1 systems, including for legacy 911 networks, transitional 911 networks, and Next Generation 911 (March 2020)
- Identify security risks in legacy 9-1-1 networks, transitional 9-1-1 networks, and NG9-1-1 networks and recommend best practices to mitigate risks in these three areas (September 2020)

[13] Section 13.5 of the CSRIC VI Report on Recommendations for 9-1-1 System Reliability and Resiliency during the NG9-1-1 Transition (March 8, 2019). https://www.fcc.gov/files/csric6wg1finalreport030819pdf

- In addition, CSRIC VII will place the vulnerabilities on a scale that accounts for both risk level and remediation expense. (March 2021)

The first two reports were delivered to the Commission in 2020. This third and final report will focus on the third item.

5 Analysis, Findings and Recommendations

5.1 Analysis

As previously mentioned by CSRIC VI, "The public safety community must continually identify risks and address evolving physical and cybersecurity requirements."[14] Because that point is vitally important to the ongoing effectiveness of 9-1-1 services, CSRIC VII's September 2020 Report on 911[15] determined there is a need to encourage and support Public Safety decision makers to provide funding to do risk assessments (initial and ongoing), perform constant cybersecurity monitoring and mitigation techniques, as well as provide ongoing support for remediation activities when needed. One approach to this is to demonstrate the impacts of cyberattacks against public safety entities (PSAPs / ECCs) and provide actionable information regarding available mitigation strategies that can be used to ameliorate or eliminate the consequences of such attacks.

5.1.1 General Impacts of Cyberattacks

In general, here are some facts that support the need for mitigation against cyberattacks irrespective of industry sector (meaning it is clear from the facts that cyberattacks are real, injurious to commerce and government, and it is not just public safety that needs to "take heed" about the need to be vigilant against cyberattacks). Public safety is not immune from this state of affairs, and the general cyber-environment today can be a dangerous threat to the normal functioning of businesses and government entities of all kinds and types.

- Ransomware may have cost the US more than $7.5 billion in 2019 https://www.technologyreview.com/2020/01/02/131035/ransomware-may-have-cost-the-us-more-than-75-billion-in-2019/
- Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021 https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

[14] *See* CSRIC VI Report on Recommendations for 9-1-1 System Reliability and Resiliency during the NG9-1-1 Transition (March 2019).
[15] *See* CSRIC VII Report on Security Risks and Best Practices for Mitigation in 9-1-1 in Legacy, Transitional, and NG9-1-1 Implementations (September 2020).

- A reference from the National Association of Insurance Commissioners talking about Ransomware and Insurance
  https://content.naic.org/cipr_topics/topic_ransomware.htm

5.1.2 Impacts of Cyberattacks Against Public Safety Entities

- Ransomware: Township confirms computer system hacked; Township hit by ransomware attack.
  https://www.erienewsnow.com/story/42683939/millcreek-township-confirms-computer-system-hacked-erie-news-now-uncovers-township-hit-by-ransomware-attack
- Brute force attacks have been successful at stealing private data (criminal data).
  https://www.southernminn.com/faribault_daily_news/news/state/article_855d63fd-08cd-5e99-84b7-0a45d234a86b.html
- Data Loss: Personal info of Minn. law enforcement, critical infrastructure personnel published online after massive hack.
  https://www.southernminn.com/faribault_daily_news/news/state/article_855d63fd-08cd-5e99-84b7-0a45d234a86b.html

  Sheriff's office hacked; "highly sensitive" information stolen.
  https://sciotovalleyguardian.com/2020/10/06/ross-co-sheriffs-office-hacked-highly-sensitive-information-stolen/
- TDoS attacks have been successful in bringing down emergency and non-emergency phone lines at PSAPs.
  - Cyber criminals tying up emergency & non-emergency phone lines through TDoS attacks
    https://www.infoworld.com/article/2614013/cyber-criminals-tying-up-emergency-phone-lines-through-tdos-attacks.html
  - Twitter originated attack in 2016, ongoing attacks from offshore bad actors, etc. Young hacker arrested for disrupting 911 Service with a TDoS attack
    http://securityaffairs.co/wordpress/52895/cyber-crime/911-service-attacks.html
- Harassment, Annoyance, SWATTING, and Accidental calls
  - *Harassment*

    Chicago police officers' radios crackled with rogue messages during weekend of chaos
    https://chicago.suntimes.com/2020/6/1/21277567/chicago-officers-radios-rogue-messages-anti-cop-music-pro-cop-slogans-during-george-floyd-protests
  - Annoyance

    Surprise Police Dept. 911 Services Hacked by 18yr Old Man
    https://www.mcso.org/Multimedia/PressRelease/911%20Cyber%20Attack.pdf
  - *SWATTING*

What is swatting? Unleashing armed police against your enemies
https://www.csoonline.com/article/3573381/what-is-swatting-unleashing-armed-police-against-your-enemies.html

Police field second swatting call in a month
https://www.hngnews.com/sun_prairie_star/news/article_bbe08764-6a85-5393-8358-4183903b8669.html

- Accidental
http://www.circleid.com/posts/20161029_teenager_arrested_for_accidental_ddos_attack_on_911_system/

5.1.3 Quantifying Cyber Risk

The need to manage cyber risk is more pressing than ever. According to the World Economic Forum's The Global Risks Report 2018, cyberattacks rank No. 3 among the top ten risks for businesses in terms of likelihood, outranked only by extreme weather events and natural disasters. In terms of impact, cyberattacks didn't even make the list in 2017— but today cyberattacks is listed at No. 6. In the World Economic Forum's, *The Global Risks Report 2021*[16], cybersecurity failure ranks No. 4 among the top ten "Clear and Present Dangers" for businesses. As cyber risk grows, so does the need to quantify it. If you can't quantify risk, how can you calculate how much cyber insurance you need? Or prioritize investments in security controls based on where you see the most risk? Or calculate the return on those investments?

5.1.3.1 Benefits of Quantifying Cyber Risk

- **UNDERSTANDING THE BUSINESS IMPACT OF RISK:** Quantification of cyber risk makes it possible to see risk in terms of its potential business impact on customer base, share price and other typical measures of business value.
- **PRIORITIZATION OF RISKS AND CONTROLS:** Effective cyber risk management depends on being able to identify and focus on the most critical risks, i.e., those that are most likely to occur and to have the greatest impact.
- **ACCURATE RISK ANALYSIS:** Cyber risk quantification is a valuable tool for a variety of risk analysis scenarios, from performing cost-benefit evaluations on risk treatments to calculating the effects of technology or business changes on the organization's risk profile.[17]

  Historically, organizations across industries have been prone to make decisions about cybersecurity on the basis of fear after an especially damaging breach or theft—without considering the trade-offs involved. Complicating this decision-making are two realities: cyberattack prevention is expensive and it's often ineffectual, since organizations can't know if, when, and how an attack might occur.

[16] See World Economic Forum (WEF), The Global Risks Report 2021, 16th Edition, p. 11. Retrieved 3 February 2021 at https://www.weforum.org/reports/the-global-risks-report-2021 .
[17] From: *RSA* Security – *3 Essentials for Cyber Risk Quantification*,
See: 3-essentials-for-cyber-risk-quantification.pdf (rsa.com)

To overcome these challenges, organizations need to take a step back to better understand their control framework and organizational challenges in detail, and then consider which remediations will give them the best outcomes. They need to know which set of initiatives to invest in and how best to choose between competing projects, and they need to accomplish all this while attacks are constantly and rapidly evolving.

For cybersecurity as for any other threat, organizations need to be able to effectively quantify the risk itself, the return on investment from addressing it, and why it may be superior to the return on other projects competing for the same resources. Certainly, chief information security officers (CISOs) would like to invest everywhere they see a threat, observe a gap, and can formulate a potential remedy, but they are forced to make trade-offs based on either their business judgment or a prescribed set of rules.

5.1.3.2 Impediments to Adequate Cyber Risk Quantification and Management

In general, researchers have identified seven "fault lines" that impede organizations' strategic thinking and ability to effectively allocate their cybersecurity investment.

1.) LIMITED INSIGHT INTO KEY IT ASSETS, THREATS, AND THE CONTROL FRAMEWORK

Organizations often lack a defined process for assessing cyber risk or understanding threats and how these might manifest—such as through unpatched vulnerabilities on phones. Insights into an organization's control framework are often limited as well, with knowledge scattered across the organization and the actual status of controls not documented. Many organizations rely on newsletters and updates from security vendors rather than performing regular, independent investigations into the areas where they may be most vulnerable.

2.) FAILURE TO PRIORITIZE CYBERSECURITY

Except when a material breach pushes cyber risk to the top of the leadership's agenda, cybersecurity and the CISO tend to occupy a peripheral position, disconnected from IT product development, digitization, and operations in most organizations.

3.) A FOCUS ON IDENTIFICATION AND PREVENTION OVER DETECTION AND RESPONSE

Security measures are useful mainly in protecting against untargeted attacks. Given the practical impossibility of achieving impermeability from determined assailants, however, reliable information security must also include detection and response. Yet, these processes are often missing from organizations' risk-management frameworks.

4.) FAILURE TO HIRE TALENT

The knowledge necessary to tackle threats and sustain operational capabilities is scarce, and organizations often struggle to attract and retain needed talent.

5.) WEAK THIRD-PARTY MANAGEMENT

Organizations are increasingly outsourcing the acquisition and management of IT assets

and cost control and integrating third-party tools into their digital ecosystems. Yet many don't know how their IT partners work, and few have the systems, resources, and protocols to oversee and monitor the work of those vendors.

6.) LACK OF A SECURITY-AWARE CULTURE

Organizations need a culture in which the institution as a whole— not just its risk owners, risk managers, and audit functions—takes responsibility for reducing information-security risk, encourages collaboration, and builds systemic resilience. Often, however, systematic accountability from the leadership to the front lines is missing or poor, and sole responsibility for information security falls on the CISO.

7.) OPERATIONAL STRESS

As attacks and incidents accelerate, organizational capabilities come under extreme pressure, often leading to systemic breakdowns and accumulating backlogs. Among the culprits: limited knowledge resources; lack of codified incident management processes; insufficient technology to monitor, log, and react to suspicious activity; and an inability to integrate technology and human capabilities.[18]

5.1.3.3 An Example of Quantifying Cyber Risk - Enterprise Cybersecurity Ratings

The quantification of cyber risk is no longer the exclusive domain of (cyber) insurance companies and academia. Utility companies, banks, corporations, and governments are increasingly using quantification approaches as part of their business and/or risk management. Across the globe, more and more organizations are reaping the benefits of these cyber risk quantification approaches to efficiently limit their cyber risk exposure. In some cases, such as insurance, this primarily concerns third-party cyber risk. In other cases, such as large banks, this concerns the management of cyber risk within the organization. For multinational companies, it concerns a combination of both. A number of different methodologies and tools are now available that range from sophisticated cyber risk benchmarks to management-oriented approaches. The uses range from threat and technology-oriented approaches to business value-oriented approaches. The paragraphs below will discuss considerations surrounding the use of cyber risk quantification modeling techniques.

As a traditional means of risk management, some have resorted to tools such as benchmarks, assessments, certifications, and norms to obtain insight into their own cyber risk posture and where to improve. However, most such approaches quickly become outdated due to the tremendous rate of change in the threat landscape. The only way to deal with this rapid change is to build the assumption of change into the framework by going to a higher level of abstraction. Unavoidably with this approach, there will always be room for interpretation, meaning that the application and interpretation will vary widely from one organization to another, leading to varying levels as well as diversification of cybersecurity.

Problems with cybersecurity have become all-pervasive because of the connectedness of technologies. As a result, more and more organizations are including third-party risk management as an important part of their cyber risk strategy. In response to this need, and in response to the actuarial needs of cyber insurance underwriters, enterprise cybersecurity ratings

[18] *A Smarter Way to Quantify Cybersecurity Risk*, Cybersecurity And A New Model for Quantifying Risk | BCG

systems have emerged in recent years. Similar to the FICO® Score for consumer credit risk, such ratings systems, including FICO® Enterprise Security Scores, aim to provide a numerical score that captures the cybersecurity posture of an organization. These systems typically use a combination of data points collected or purchased from public and private sources and proprietary algorithms to articulate a rated company's security effectiveness into a quantifiable measure or score. While the efficacy of a security program cannot be solely reduced to a single number, security ratings based on accurate and relevant information are useful tools in evaluating risks. And, as security rating technology continues to mature, more organizations in the public and private sectors will leverage these scores for making business and risk decisions.

A ratings system plays two very important roles. Like a consumer credit rating, an enterprise security rating introduces a potentially standard and normalized way of inspecting the security posture of a third party or a peer. In addition, it can serve as a way for an organization to self-evaluate and self-regulate. For instance, it could be used to gauge the effectiveness of resource allocation strategies in cybersecurity within an organization. Against the backdrop of the high degree of connectedness of cybersecurity, such ratings systems are critical to the cybersecurity ecosystem as a tool to assess the security conditions of those connected to each other. As rating technology matures, it is important that rating companies work toward standardization and transparency of these rating systems. Both can help various stakeholders in the ecosystem reach a common understanding of the meaning of cybersecurity ratings and common practices for how they are used in areas such as vendor validation and underwriting.

5.1.3.4 A Note about Systemic Cyber Risk

As the discussion about third party risk above indicates, cyber risks are widely perceived to be intrinsically systemic and there is no question that this is true. Even for, and perhaps especially for, public safety, cybersecurity risk introduced into the 9-1-1 system through the adoption of NG technologies sets up an interconnected system of technologies and capabilities that are at risk in total, and not just at the individual PSAP/ECC or Governing Authority level. Look at a survey by AIG sent to a global group of experts indicated that more than 90% believe that cyber risk is systemic, across ALL sectors of government and industry. Approximately 60% saw a 50% or greater chance of a multi-organization event in the subsequent 12 months, with over half noting a 10% or greater chance of an event impacting 50–100 organizations. In fact, with the benefit of hindsight, it appears that the experts may have underestimated the potential for a systemic event.

In general, recent research has observed four types of systemic cyber risk scenarios:

1. *Common vulnerabilities* – Widespread vulnerabilities that lead to the risk of rapidly spreading malware infections and associated abuse (such as the Mirai, WannaCry and NotPetya attacks).

2. *Infrastructure failure cascade* – A cyberattack that causes the failure of a single organization or infrastructure service provider may have a cascading impact on many other organizations that rely on that infrastructure (such as the Ukrainian power grid, Dyn DNS services, Amazon S3 outages and CloudFlare CDN vulnerabilities).

3. *Trust-base* – A loss of integrity undermines trust-based value systems, e.g., financial, news media or democratic systems (such as the SWIFT-related attack on the Central

Bank of Bangladesh).

4. *Indirect attacks* – Attacks that exploit third and even fourth parties to reach large, higher-value targets imply an unmanageably large attack surface (such as the fallout from NotPetya for Maersk, the attack on the relatively small HVAC supplier that led to the Target breach, and the compromised vendor credentials used to exploit Equifax's vendor portal that led to massive data breaches).

PSAPs/ECCs and other public safety entities have strong intrinsic motivation to limit their own cyber risk, but as research indicates, this cannot be done without paying attention to the systemic risks inherent in the transition to NG9-1-1. [19]

5.1.3.5 A Methodology for Quantifying Cyber Risk

The following paragraphs discuss a top-level methodology, used by industry practitioners (this example is borrowed from RSA Security, an industry leader in cybersecurity technology) on how to make cyber risk more quantifiable:

1.) DEFINE RISK PRECISELY

A fundamental problem with many methods for measuring cyber risk today is that they use basic terms like "risk" and "threat" imprecisely and inconsistently. This makes it difficult to measure risk reliably or communicate about it effectively. The FAIR Institute, which promotes the Factor Analysis of Information Risk (FAIR) framework for measuring cyber risk, argues for defining risk more precisely by viewing it in terms of potential loss events—for example, a malicious breach of sensitive consumer or corporate information, cyber theft of intellectual property or destruction of critical data. These specific loss-event scenarios differ significantly from more general descriptions of risk, such as "weak passwords," "cybercrime" or "disgruntled former employees," which are really more accurately described as factors that contribute to risk. Loss events can be assessed in concrete terms, such as frequency (how likely they are to happen) and magnitude (how much impact they may have), which in turn makes it possible to measure risk more accurately and communicate about it more clearly.

[19] *Quantifying Systemic Cyber Risk*

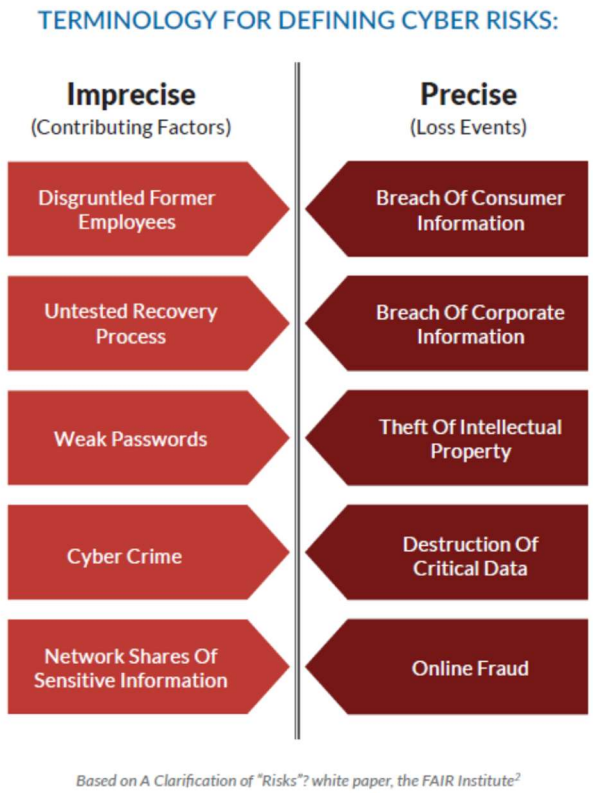

Figure 1: Terminology for Defining Cyber Risks

2.) SCOPE RISK CLEARLY

Many frameworks for defining or measuring cyber risk today assign risk ratings of high, medium, or low (often designated by color, i.e., red, yellow or green). That may seem sensible. But unless you know the underlying assumptions about those categories, you can't really understand the true scope of the risk. For example, when you say "high-risk," what do you mean by "high"? It is, after all, a relative term: Knee-high to a grasshopper is something entirely different than high as the moon. So, if you use the term without context, you don't really have an understanding of what you're measuring. The next time you hear something described as posing a high risk, ask yourself:

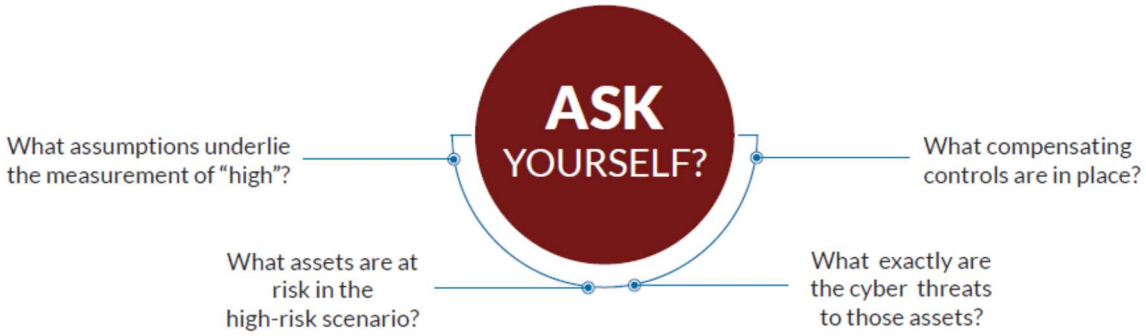

Figure 2: Scoping Risk with Precision

3.) APPLY ACCURATE MODELING

The quality of cyber risk measurement today often depends on how well the practitioners measuring the risk understand the complex array of factors in play. Cyber risk measurement is a fairly new discipline, and it shouldn't be surprising that few cybersecurity professionals are trained in its principles. Combine the lack of skills, training, and experience with the previously described problems of imprecise terminology and inaccurate scope, and you're not likely to end up with an accurate model for measuring cyber risk.

5.1.3.6 The FAIR Model for Risk Measurement

To measure cyber risk accurately, you need a new, more effective model for quantifying risk. The FAIR framework provides an open international standard risk model that was developed specifically to enable effective risk measurement. At its core, FAIR is a risk calculation model that overcomes issues of imprecision and lack of scope by specifically taking into account loss events, their likelihood, and their magnitude

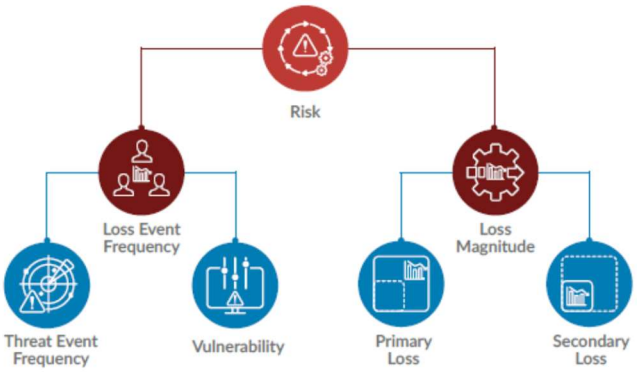

Figure 3: Factor Analysis of Information Risk (FAIR) Model

FAIR addresses several of the shortcomings of existing approaches to risk measurement in the following ways:

- Defines risk factors clearly and completely to reduce imprecision and confusion

- Takes into account the mental models of those tasked with measuring risk to help ensure accurate scoping and measurement
- Provides a framework for critical thinking to lessen the chance of overlooking key factors
- Enables robust quantitative analysis using established methods
- Can be applied using a triage approach to quickly establish priorities for risk treatment or as part of a more in-depth, long-term risk management plan [20]

CSRIC VII recommends public safety personnel responsible for cybersecurity employ methodologies like the Factor Analysis of Information Risk (FAIR) Model to quantify their cyber-risk profile and corresponding mitigation and remediation strategies. What may seem the most appropriate use of limited resources to ensure cybersecurity protection for public safety entities migrating to NG9-1-1 may not indeed be that once a quantitative cyber risk analysis is performed.

5.1.4 9-1-1 Fees and Cybersecurity

Prior to providing recommendations on 9-1-1 fees relative to cybersecurity investments, CSRIC notes some recent developments at the FCC and in Congress. The Commission recently published its annual 9-1-1 fee report, which included data from states about 9-1-1 cybersecurity expenses and whether 9-1-1 fees had been used to fund cybersecurity.[21] CSRIC also notes provisions in the December 2020 Omnibus budget bill that prohibit 9-1-1 fee diversion at the federal level and sets up a special public/private "strike force" under the Commission to advise on mechanisms that should be instituted to prevent or mitigate 9-1-1 fee diversion, up to criminal penalties.[22] The following analysis is provided in the context of both the annual 9-1-1 fee report and this legislation.

5.1.4.1 The FCC Should Collect Information on Cybersecurity Maturity Levels

The Commission notes in the Fee Report that most states did not report spending 9-1-1 funds on cybersecurity (34 states and 4 territories reported on this)[23] and most respondents reported zero or an unknown number of PSAPs participating in a cybersecurity program.[24] Of course, the conclusion that no 9-1-1 funds were spent on cybersecurity in these 38 states and territories is questionable, and the Fee Report does not imply this. Even low-tech, staff education in cybersecurity hygiene procedures are a form of cybersecurity expense as noted in this report, and any modern technology system employs some sort of cybersecurity mechanism. The Fee Report acknowledges this, noting that nearly half of respondents simply could not answer the

[20] From: *RSA* Security – *3 Essentials for Cyber Risk Quantification*
[21] See Twelfth Annual Report to Congress on State Collection and Distribution of 911 and Enhanced 911 Fees and Charges. Retrieved 21 December 2020 at https://www.fcc.gov/files/12thannual911feereport2020pdf ("Fee Report").
[22] See United States Consolidated Appropriations Act, 2021, Title IX at Sec. 902. Retrieved 21 December 2020 at https://rules.house.gov/sites/democrats.rules.house.gov/files/BILLS-116HR133SA-RCP-116-68.pdf ("2020 Budget BIll").
[23] See Fee Report at 4.
[24] See Fee Report at 49.

question.[25]

The FCC's annual fee reports are valuable information for the 9-1-1 community, and a comparative assessment of organizational cybersecurity maturity included in the fee report could be used to justify future investments in cybersecurity programs or even federal legislation and may also be helpful in building the case to end 9-1-1 fee diversion. Going forward, the FCC should include cybersecurity maturity as a question of inquiry in its annual Fee Report.

5.1.4.2 9-1-1 Fee Diversion Meaningfully Threatens 9-1-1 and NG9-1-1 Security

In implementing the provisions of the 2021 Budget Bill, CSRIC notes the Commission will be called upon to convene the *Interagency Strike Force to End 9-1-1 Fee or Charge Diversion*.[26] The FCC reports about $3 billion USD in 9-1-1 fees was reported to be collected for the calendar year ending December 31, 2020, and about 9.2% (about $278 million USD) of which was reported diverted for other purposes.[27]

9-1-1 fee diversion can harm 9-1-1 cybersecurity planning, as any money diverted from 9-1-1 obviously cannot be invested in improving 9-1-1 security. The group notes a recent Kaspersky Report of small-to-medium businesses which relates that 10% of small-to-medium businesses plan to *reduce* funding for cybersecurity in the next year.[28] Particularly in light of a modest budget year following the COVID-19 pandemic, CSRIC notes that many state and local governments have struggled to make ends meet and balance their budgets for FY 2021. The Center for Budget and Policy Priorities reports that tax revenues through the pandemic have been over 6% lower than the previous year when normally most localities would have planned for them to increase by 2-3%,[29] and in some localities, 9-1-1 fees may be an attractive target to address budget shortfalls. The Commission, even under the new authorizing statute in the 2021 Budget Bill, can do very little to compel states and localities to not divert 9-1-1 fees to other purposes; however, it should continue doing everything in its power to monitor and report on the issue.

5.1.4.3 Cybersecurity Investments should be Normal and Customary 9-1-1 Spending

CSRIC notes that conventions for what is eligible for 9-1-1 funding varies widely; collection methods vary (whether collected by the state or county), as do determinations for eligible expenses; also, fee amounts vary widely (and sometimes do not exist at all or do not actually fund 9-1-1 service). Clearly, 9-1-1 fees should be spent on 9-1-1 service; and CSRIC affirms this widely held position. However, cybersecurity may not be explicitly supported as an eligible expense. As should be clearly justified by this and previous CSRIC VII reports, cybersecurity is a core and fundamental part of implementing and managing a 9-1-1 or NG9-1-1 system, and so, should not be considered as a separate investment. As part of its upcoming work, the Commission should ensure that cybersecurity expenditure is defined as not only an acceptable

---

[25] See Id.
[26] See 2020 Budget Bill at Sec. 902(d)(3).
[27] See Fee Report at 2.
[28] See https://usa.kaspersky.com/about/press-releases/2020_2020-it-spending-cybersecurity-remains-an-investment-priority-despite-overall-it-budget-cuts-kaspersky-found, retrieved 21 December 2020.
[29] See *States Grappling With Hit to Tax Collections*, Center for Budget and Policy Priorities, retrieved 21 December 2020 at https://www.cbpp.org/research/state-budget-and-tax/states-grappling-with-hit-to-tax-collections.

use of collected 9-1-1 funds but is also considered an encouraged use of such monies.

5.2 Findings

5.2.1 What can be done to mitigate the impacts of cyberattacks?

NOTE: Cost estimates associated with these items begins at section 5.2.2.1.

As the technology evolves, leadership is strongly encouraged to review funding allocation decisions to ensure that cybersecurity investments keep pace with technology innovations. The communications technology required to support the NG9-1-1 infrastructure is adding new hardware elements and software functionality at an unprecedented pace, including many features that address existing security threat vectors and/or secure known vulnerabilities. However, with each new addition comes the high probability that a new cyber threat is also enabled. In some cases, this includes the very features originally implemented to secure the NG9-1-1 system in the first place.

Examples of cyber threats are brought to our attention daily via national news media. If leaders and their staffs do not fully understand the risks and ways to mitigate them, they are encouraged to retain the services of industry experts to assist in planning organizational approaches to addressing the cyber threat issue. These same industry experts can assist in recommending budget changes that may be required to support efforts to protect NG9-1-1 operations.

As a prerequisite to implementing any of the controls described in this document, *every* organization in the public safety service value chain, including vendors that provide information technology solutions must identify a Chief Information Security Officer (CISO), an individual whose responsibility is to work on cybersecurity for the organization. This individual should ideally be a dedicated employee but may be an employee who has additional duties or a contractor. This individual must be responsible and be held accountable for improving the cybersecurity posture of the organization, whether by doing the work himself/herself, oversees other employees doing the work, or oversees vendor contracts for these services. This applies whether an entity is doing all or some of the following steps internally or utilizing a third party to perform them.

It should be noted that there may be barriers to implementing one or more of the mitigations described below. Aside from costs, barriers to implementation of the mitigations may include local governance that limits the agency's ability to perform one or more of the identified cyber mitigation functions. Such governance can be affected by ownership of the platform elements. For example, a county or state may manage the IP infrastructure used by the PSAP/ECC, which could impede the PSAP/ECC from performing the tasks. Another potential barrier could be regulations or laws that preclude the agency’s ability to perform the mitigation tasks, such as the Criminal Justice Information Services (CJIS) password rules.

Also note that outside commitments may compel an organization to adjust the performance frequency of the mitigation and remediation strategies discussed above. For example, organizations operating a certificate authority are subject to strict independent audit requirements according to specific guidelines outlined in a certificate policy and certificate practice statement. Additionally, cyber-insurance plans generally have requirements that the

insured must adhere to in order to maintain coverage, such as implementing certain cybersecurity best practices. Further, CJIS compliance policies may impact cyber practices, such as password policies. The guidelines below are provided as a baseline and do not supersede any requirements an organization is bound to by its existing policies, contracts, and agreements.

Given the mission critical nature of 9-1-1 it is imperative that all mitigation techniques are designed and staffed to be accomplished in a timely manner, respecting the 24x7x365 nature of the mission.

- The single-most comprehensive solution is continuous cyber monitoring. Agencies with limited cyber budgets should, at a minimum, support this solution. https://transition.fcc.gov/pshs/911/TFOPA/TFOPA_FINALReport_012916.pdf and https://transition.fcc.gov/pshs/911/TFOPA/TFOPA_WG1_Supplemental_Report-120216.pdf
- Vulnerability assessments should occur at a minimum of every 90 days across the whole of the infrastructure. CSRIC VII recommends weekly scans of externally visible network space are recommended. Tools should be updated as frequently as possible, but not less than once a week.
  https://www.fcc.gov/document/fcc-releases-tfopa-final-report (page 211)
  However, if the type of cyber monitoring supported provides weekly reports and regular external analysis, then vulnerability assessments could instead be done annually.
- Have three (3) backups on two (2) different forms of media storage (such as cloud, tape, external drive, flash drive) that can be connected for use on demand. Do not allow any of them to be connected to any network or system until needed. One of the backups must be stored offsite, and geographically & logically separated from the others.
  https://www.nccoe.nist.gov/sites/default/files/library/supplemental-files/msp-protecting-data-extended.pdf (see the bottom of page 2 of that document)
  and
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf#page=29

  Note that auto-syncing cloud services do not constitute a full backup, even though they are often marketed as such both to private individuals as well as to large enterprises. These services replicate a copy of data locally and via a cloud service. It is true that these services do protect from the loss of data through loss of a device, such as if the device is destroyed or experiences hardware failure. These services also allow for rapid restoration, because even if an end-user device is destroyed, the data can simply be accessed and provisioned onto a replacement device.

  However, these services do not protect from other forms of data compromise. For example, if data is altered maliciously, those alterations will be replicated in the cloud. If data is corrupted, the corruption will be replicated in the cloud. Or if information is simply deleted, whether by accident or by a malicious user, the remote copy will be lost as well, as the cloud service will replicate any local changes as it is designed to do, which in this case is to delete the copy of the file on the cloud—deleting the "backup". Accordingly, cloud-syncing services should NOT be considered a comprehensive form of backup, and do not necessarily satisfy the recommendation above to provision three

backups of any critical data.

- Have a written cyber response plan in place and test it at least quarterly to ensure you can recover from your backups. Spot check each backup for consistency and viability to know it saved correctly. Quarterly testing of backups by using a backup PSAP is a safe way to accomplish this task.
  NIST Special Publication (SP) 800-184 Guide for Cybersecurity Event Recovery
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf#page=29
- Have affirmative coverage cyber insurance.[30] Use it to pay for third party assistance to aid with recovery. DO NOT use it to just pay the ransom. Be sure in advance that your third party cyber-expertise vendor is approved by your insurance provider.
  https://www.cisa.gov/cybersecurity-insurance

  Some of the other reasons for not paying ransom include:
  1. You are funding cyber criminals
  2. You may be funding terrorists (see Office of Foreign Assets Control[31] rules)
  3. You've just identified yourself as a viable revenue source for the hacker
  4. You may not get your data back anyway
  5. You may (probably will) be attacked again by a different hacker.
- Get the best firewall you can afford. Costs are usually dependent upon the number of ports, but costs can vary widely.
- Use network segmentation and put sensitive info behind additional firewalls.
  NIST "A Guide for Managed Service Providers to Conduct, Maintain and Test Backup Files" https://www.nccoe.nist.gov/sites/default/files/library/supplemental-files/msp-protecting-data-extended.pdf
- Limit user privileges to only what is needed to accomplish each specific job's duties.
  NIST Special Publication 800-184 Guide for Cybersecurity Event Recovery
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf#page=29
- Cyber-hygiene training should be provided to all staff members, including training to identify Phishing attacks, and the proper use of the agency's network for web surfing, personal email use, accessing social media, etc. Such training could include ongoing phishing simulations[32] and subsequent remediation training at a group or individual level.
- Provide cyber-safe methods for staff members to perform personal tasks that are inherently necessary in the course of telecommunicator work responsibilities. These

[30] One such example is Georgia's Cybersecurity Insurance policy information:
http://doas.ga.gov/risk-management/insurance-services.
The actual policy is located at:
http://doas.ga.gov/assets/Risk%20Management/Liability%20Insurance%20Publications%20and%20Forms/DOAS%20Cyber%20XL%20Catlin%2007012017.pdf
[31] Office of Foreign Assets Control: https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information
[32] https://en.wikipedia.org/wiki/Simulated_phishing

incidental mitigation techniques for non-intentional impacts include providing individual separate Universal Serial Bus (USB) charging stations or equivalent methods (data blocker dongles) to charge personal phones/tablets, establish a guest network (either managed or outside of the emergency services network) to accommodate Bring Your Own Device (BYOD) usage, disable the local USB ports (at a user privilege level if possible), etc.

- Protect remote access by using secure methodology that is updated to the latest version and meets or exceeds the minimum standard (NIST SP 800-53)[33] of password creation and storage and also utilizes a multifactor authentication methodology.
- Guarding the Confidentiality, Integrity & Availability (CIA) of location data on 9-1-1 calls is important. When an industry supported mechanism, comparable to the signing/verification mechanism (SHAKEN) that has been specified for caller identity information becomes available for location information, support of that mechanism by network providers would allow a PSAP call taker to better assess the degree to which the location information provided with a 9-1-1 call can be trusted.
- If anycast DNS is utilized, secure it by incorporating a methodology that protects the dynamic routing from being hijacked, by utilizing an enterprise level DNS protection service.

5.2.2 Estimated Costs to Mitigate the Impacts of Cyberattacks

5.2.2.1 Estimated cost of Chief Information Security Officer (CISO)

Cost ranges for a CISO vary widely depending on the level of work involved, and geographic location. The ranges shown below are at full-time/part-time, internal, outsourced, salaried, monthly, and hourly rates. For example:

- According to talent agency Mondo's 2020 salary guide, the range for a CISO is between $175k-$300k.
- According to Ongoing Operations the monthly ranges are $4.5k–$12k each month. https://ongoingoperations.com/2020/02/18/ciso-service-cost/
- According to ATLANT Security the hourly range is $100-$200 depending on the size of the project. https://atlantsecurity.com/ciso-as-a-service/

5.2.2.2 Estimated Costs of Continuous Cyber Monitoring

The costs & time required for any size organization to build (or add-to) cybersecurity continuous monitoring capabilities are significant. As the cybersecurity industry is ever evolving, keeping a Security Operations Center (SOC) up-to-date and state-of-the-art can put great pressure on annual IT operating budgets.

When considering building and maintaining a stand-alone SOC capability, at a minimum, the following needs to be considered:

[33] NIST Security and Privacy Controls (NIST SP 800-53): https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

- **Staff:** Based upon experience in the public safety sector by CSRIC participants, seven is the minimum number of cyber staff required to effectively provide 7x24x365 cybersecurity monitoring. The current market demand for this talent requires a focused human capital (recruit, retain, grow, salary, etc.) effort above and beyond that of other IT staff. The entire financial burden (hard and soft costs) of staffing a SOC rests with the organization.
    - Cost: hundreds of thousands of dollars per year
- **Tools:** State-of-the art tools are required to provide effective cybersecurity monitoring. Cost associated with selection, procurement, training, upgrades, annual maintenance costs, etc. – all need to be factored into the cost analysis.
    - Cost: tens of thousands of dollars per year
- **SOC Facility:** Unlike a traditional Network Operations Center (NOC), a Security Operations Center (SOC) is a location that focuses exclusively on carrying out the security functions of an organization. The efficiency and effectiveness of a SOC is critically dependent on the physical space being dedicated to that mission, along with workspace for the cyber talent, equipment, and tools. Initial cost of securing such a space, filling it with furniture, technology, etc. must be factored into the planning and budgeting process.
    - Cost: tens if not hundreds of thousands of dollars per year (more in first year)
- **Annual Operations:** The cyber industry is incredibly dynamic and fast-paced. As a result, a SOC (staff, tools, equipment, space, etc.) must be continually maintained and updated. Annual budgets to upgrade the center's capability must be addressed in addition to the annual SOC operating budget.
    - Cost: hundreds of thousands of dollars per year

- Estimated Total Cost: ~$1,000,000+

Cost Analysis Breakdown to Build a Security Operations Center (SOC)

SOC Staff (8 people)	
Senior Cyber Manager[34] (1 person)	$116,066.00
Cyber Analyst[35] (7 people)	$606,501.00
SOC Employee Benefits[36] (8 people)	$235,406.14 (~32%)
Tools[+37]	~$20,000

[34] $116,066 US National Average Senior Cybersecurity Manager (n=2111): https://www.glassdoor.com/Salaries/senior-cybersecurity-manager-salary-SRCH_KO0,28.htm
[35] $86,643 US National Average Cybersecurity Analyst (n=4225): https://www.glassdoor.com/Salaries/cybersecurity-analyst-salary-SRCH_KO0,21.htm
[36] In the US, about 30% of total employee compensation is benefits: https://www.bls.gov/regions/southwest/news-release/employercostsforemployeecompensation_regions.htm
[37] The + and ~ symbols indicate an approximate minimum level of investment required to provide basic level of SOC services.

SOC Facility[+]	~$50,000
Annual Operations[+]	~$150,000
Total Cost Per Year	~$1,000,000+

Additionally, for further information, salaries for a variety of analogous job titles that may fulfill the roles listed above are included in Mondo's 2020 salary guide. Organizations should consider these job titles and the associated costs when budgeting for their cybersecurity programs. Actual compensation and fully loaded personnel costs may vary depending on market conditions in a given locality as well as specialization of a given role, but these rates may assist in identifying an order of magnitude for staffing cybersecurity programs for 9-1-1 organizations.

From the Talent Agency Mondo's 2020 Salary Guide

Position	Low ($k)	High ($k)
Application Security Engineer	120	180
Compliance Analyst	80	125
Cybersecurity Engineer	120	200
Cybersecurity Analyst	90	160
Information Security Analyst	85	125
Manager, Information Security	125	215
Network Security Administrator	85	120
Network Security Engineer	125	180
Security Operations Center Analyst	75	145

5.2.2.3 Estimated Costs of Vulnerability Assessments

Based upon experience in the public safety sector by CSRIC participants, cost ranges for vulnerability assessments are between $8.5k-$90k per assessment, per PSAP. This cost will vary based upon the design and size of the network and the approach and type of techniques used to conduct the assessment.

5.2.2.4 Estimated Costs of the prescribed backups

Ranges are between $2 to $4 per month per gigabit of memory used.
https://resource.optimalnetworks.com/blog/2015/03/31/cost-data-backup-small-business#:~:text=What%20is%20the%20average%20price,for%20lower%2Dlevel%20data%20backup.

5.2.2.5 Estimated Costs of Having a Written Cyber Response Plan

Simply stated, the cost of not having a cybersecurity plan is potentially based upon the cost of a single human life. 9-1-1 is an essential life safety service and the cost of a cybersecurity event could very well be the loss of human life. This should be viewed as unacceptable.

The cost of developing a cyber-response plan is justifiable on a purely statistical basis.
CSRIC notes that the cost of a single human life is priceless. However, the Commission and other regulatory entities have attempted to estimate the statistical value of a human life; the

Commission has recently used a Value of Statistical Life (VSL) set at $9.6 million USD in justifying the cost of past regulatory activity.[38] CSRIC notes that it is difficult to exactly quantify the likelihood that, as a consequence of a cyber event, that one or more human lives will be lost; it is further more difficult to quantify exactly the likelihood that one or more individuals will be injured or otherwise experience loss, but not lose their lives due to a cyber event and to quantify the exact associated costs.

However, jurisdictions may consider VSL when determining which level of funding for a cyber response plan is appropriate, considering that simply having some sort of response plan in the first place is one of the foundational steps towards responding to cyber events that will happen in the future. This is above and beyond evaluating financial outlays due to more immediately obvious costs, such as insurance deductibles, hourly costs associated with external experts and other costs.

While it is difficult to estimate the total costs of writing a response plan without knowing the specifics of a given organization, the following budgetary ranges are provided for planning purposes; these numbers assume the following:

- One or more dedicated external experts are assigned to the project
- Project management and stakeholder overhead is not included (assume approximately 10%-20% increase an hour to account for project management and stakeholder involvement)
- Hourly rates roughly in accordance with industry rates[39]
- Approximately 10% annual effort retained each year to update and maintain the document.

	Small Organization (~10 employees)	Medium Organization	Enterprise	Large Enterprise
Hourly Rate	$250	$200	$150	$150
Hours, Initial Drafting	160	540	1080	4160
Total Capital Costs:	$40,000	$108,000	$162,000	$624,000
Annual Maintenance:	$4,000	$10,800	$16,200	$62,400

[38] See *Report on the National Suicide Hotline Improvement Act of 2018*, United Stated Federal Communications Commission, Wireline Competition Bureau, Office of Economics and Analytics, 14 August 2019 at pg. 17: "The VSL is currently $9.6 million—meaning that people, on average, highly value their lives and are willing to spend, for instance, one percent of this amount to reduce their mortality risk by one percent.144 In order to estimate a benefit floor, above which we expect the benefits exceed the costs, we divide the $570 million in cost reduction needed for the first year by the $9.6 million value for a statistical life for a total of nearly 60 statistical lives ($570 million / $9.6 million = 59.4)."
Retrieved 5 January 2021 at https://docs.fcc.gov/public/attachments/DOC-359095A1.pdf.

[39] See, e.g., rates available at: https://atlantsecurity.com/ciso-as-a-service/: "the price for smaller projects is higher and is around $200 an hour". This analysis assumes a medium organization contracting for one project constitutes a small project, and a discount/premium of $50/hr is applied to large and small projects. This example is used illustratively and does not constitute endorsement.

These figures are budgetary only. However, it is worth considering when justifying the cost of developing a cyber response plan that, on a purely statistical basis, it is reasonable for a medium-sized organization to initially invest $108,000 USD to write a plan and $10,800 annually to keep it updated if there is only a 0.5% chance that doing so could prevent an individual losing their life.[40]

A medium-large size PSAP can receive several thousand calls per day.[41] Every one of those calls is a potentially life-affecting emergency and must be answered promptly, safely, and securely. However, when PSAPs and 9-1-1 authorities experience trouble justifying the cost of a cyber-response plan, they may consider factors such as VSL and how their potential risk of exposure to a cyber-attack impedes their ability to process emergency calls, potentially resulting in the loss of human life.

5.2.2.6 Estimated Costs of cyber insurance

Actual premium prices would vary depending upon the type of business, location, and claims history. Logically, higher liability limits will result in higher premiums and deductibles will also impact premiums.

Factors that Affect Cyber Insurance Costs

- Size and Industry of Applicant
- Amount and Sensitivity of Data
- Annual Budget
- Strength of Security Measures
- Policy Terms
- Crisis services
    - Forensics
    - Remediation
    - Notification
    - Credit monitoring
    - Legal guidance
    - Public relations
    - Legal Damages
    - Legal defense
    - Settlement
- Regulatory Action
    - Defense
    - Fines
- Payment Card Industry
    - Fines

[40] As discussed, the VSL for a human is $9.6 million; at year 3, the estimated budgetary cost for a medium-sized organization to write and maintain a cyber response plan for a medium organization is $129,600 ($108,000 capital cost and two years' worth of maintenance at $10,800 annually).

[41] For example, Washington D.C. answered up to around 90,000 calls per month in 2018; see https://dccouncil.us/wp-content/uploads/2020/01/JPS-Performance-Oversight-Responses-2020-OUC.pdf at pg. 82.

Examples:

- **Reference 1**: Cyber Data-Risk Managers suggest the following Data Breach Insurance Cost? https://databreachinsurancequote.com/cyber-insurance/cyber-insurance-data-breach-insurance-premiums/

Industry	Operations	Limits	Premium
Political	SaaS	$10,000,000	$58,126.74

- **Reference 2:** Advisor Smith suggests the following Average Cost of Cyber Insurance https://advisorsmith.com/data/average-cost-of-cyber-insurance/#:~:text=The%20average%20cost%20of%20cyber,data%20breaches%2C%20according%20to%20IBM

  The following table uses quotes and rate filings from major insurance companies in Connecticut to demonstrate the low end of average annual premium charges for different levels of coverage with varying deductibles, based upon a business with moderate risk in the state of Connecticut.

Cyber Liability Limit	Deductible	Example Annual Insurance Premium
$1,000,000	$10,000	$1,588
$500,000	$5,000	$1,146
$250,000	$2,500	$739

5.2.2.7 Estimated Costs of firewalls

Ranges from $16,000 to $228,000 for firewalls with Next Generation N(G) capabilities and a minimum protected throughput of at least 1Gbps. Most will also have an additional annual license fee. If bandwidth needs are higher, then you need a more robust firewall, which will cost more.

5.2.2.8 Estimated Costs of using network segmentation

The cost for network segmentation is inherently embedded within the duties of a CISO or equivalent role. Part of a CISO's responsibilities is to evaluate or in some case establish the network architecture of the ECC. The desired result is to have the network architected in a manner that achieves the necessary level of cybersecurity segmentation.

5.2.2.9 Estimated Costs of limiting user privileges

The cost for limiting user privileges is inherently embedded within the duties of a CISO or equivalent role. Part of a CISO's responsibilities is to establish and maintain user privileges within the ECC. The desired result is to have limited user privileges based up their role.

5.2.2.10 Estimated Costs of Cyber-hygiene training

Based upon experience in the public safety sector by CSRIC participants, cost ranges for cyber-hygiene are approximately $249.00 per virtual seat or $5000.00 for on-site per Agency.

5.2.2.11 Estimated Costs of Phishing Simulations

Based upon experience in the public safety sector by CSRIC participants, cost ranges for Phishing Simulation training vary widely based on the methods used for training and the number of seats involved. One example is a vendor that charges $5000.00 for up to 50 seats on a yearly basis for a managed Phishing Simulation technique.

5.2.2.12 Estimated Costs of incidental mitigation techniques for non-intentional impacts

Based upon experience in the public safety sector by CSRIC participants, costs for this category are generally based on the quantity of elements involved. For example, the cost range of USB charging stations are $30-$65. The estimated range for establishing a BYOD guest network (outside of the emergency services network) $60-$100+ per month for non-managed Internet access.

5.2.3 Basic Cybersecurity Controls Which Can Be Implemented at Low Cost

As in Report 2, CSRIC VII recommends that organizations implement and follow a recognized cybersecurity controls framework. In doing so, they should evaluate where they fall along a given method's maturity continuity, which controls they have already implemented, and which are the highest priority to implement first. This report reaffirms these recommendations and notes that this may be considered a fundamental responsibility of the CISO, as discussed in section [5.2.1]. CSRIC VII also notes that basic controls can be implemented at a very low cost to organizations of any size and capability.

Cybersecurity controls are guidelines that provide a roadmap to improve an organization's cybersecurity posture. Controls generally follow the same format: it is a list of best practices, organized into maturity states and/or organizational state or cost levels. As a rule, recognized cybersecurity controls usually conform to NIST's Cybersecurity Framework (CSF) but provide practical guidelines on implementing the NIST CSF for organizations of different sizes or capabilities.

While Report 2 and this report use CIS' controls illustratively, CSRIC notes that following recognized cybersecurity controls model will improve the cybersecurity posture of an organization. Some notable examples of recognized control frameworks include the following:

- Center for Internet Security (CIS) Controls: https://www.cisecurity.org/controls/
- Department of Defense Cybersecurity Maturity Model Certification (CMMC): https://www.acq.osd.mil/cmmc/draft.html
- CERT Resilience Management Model (RMM): https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508084
- NIST Security and Privacy Controls (NIST SP 800-53): https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

For example, CIS Controls include three Implementation Groups (IG): Basic, Foundational, and Organizational. These are self-assessed categories into which an organization will determine it falls based on (1) data sensitivity and criticality of services offered by the organization, (2) expected level of technical expertise exhibited by staff or on contract and (3) resources available

and dedicated toward cybersecurity activities.[42] Of course, all 9-1-1 operations fulfill the first of these three measures, that of the sensitivity and criticality of the organization's data, as 9-1-1 operations handle sensitive medical, criminal and other data. However, it cannot be reasonably assumed that all 9-1-1 operations fulfill the second and third categories, as many organizations have limited technical expertise and financial resources.

Most of the controls included in CIS IG1, or Basic, can be implemented at little or no cost to the organization. Accordingly, as in Report 2, CSRIC recommends that all organizations implement a level of controls equivalent or similar to CIS IG1, regardless of size, capabilities, or resources.

Report 2 stated the following:

> *IG1 includes basic cybersecurity practices that apply to all organizations; basic requirements like maintaining an asset inventory or password management are reasonable requirements to apply to all organizations. This recommendation [to implement IG1 controls] applies to small ECCs all the way to very large ESInets serving thousands of telecommunicators. These practices also apply to legacy, transitional and end-state 9-1-1 and NG9-1-1 networks.*
>
> *IG1 measures are, uniformly, inexpensive and do not require sophisticated technical resources or system to implements. Most of them are procedural controls that can be included in organizational practices and training programs and are understandable by a non-technical audience. However, as the case studies included in this report detail, these vulnerabilities do exist in public and commercial spaces today. Some of these attacks can be mitigated by low-cost and easy-to-implement programs, and there are freely available training materials that cover all or most of these practices.*[43]

IG1 controls include the following:

Table 3: CIS Controls Implementation Group 1

Asset Type	Security Function	CIS #	Title	
Devices	Identify	1.4	Maintain Detailed Asset Inventory	Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not.
Devices	Respond	1.6	Address Unauthorized Assets	Ensure that unauthorized assets are either removed from the network, quarantined, or the inventory is updated in a timely manner.
Applications	Identify	2.1	Maintain Inventory of Authorized Software	Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.

[42] See CIS Controls at pg. 4. Retrieved 30 November 2020 at https://www.cisecurity.org/controls/.
[43] See CSRIC VII Report 2.

Asset Type	Security Function	CIS #	Title	
Applications	Identify	2.2	Ensure Software is Supported by Vendor	Ensure that only software applications or operating systems currently supported and receiving vendor updates are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.
Applications	Respond	2.6	Address unapproved software	Ensure that unauthorized software is either removed or the inventory is updated in a timely manner
Applications	Protect	3.4	Deploy Automated Operating System Patch Management Tools	Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.
Applications	Protect	3.5	Deploy Automated Software Patch Management Tools	Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.
Users	Protect	4.2	Change Default Passwords	Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.
Users	Protect	4.3	Ensure the Use of Dedicated Administrative Accounts	Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.
Applications	Protect	5.1	Establish Secure Configurations	Maintain documented security configuration standards for all authorized operating systems and software.
Network	Detect	6.2	Activate Audit Logging	Ensure that local logging has been enabled on all systems and networking devices.
Applications	Protect	7.1	Ensure Use of Only Fully Supported Browsers and Email Clients	Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.

Asset Type	Security Function	CIS #	Title	
Network	Protect	7.7	Use of DNS Filtering Services	Use Domain Name System (DNS) filtering services to help block access to known malicious domains.
Devices	Protect	8.2	Ensure Anti-Malware Software and Signatures Are Updated	Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.
Devices	Detect	8.4	Configure Anti-Malware Scanning of Removable Devices	Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.
Devices	Protect	8.5	Configure Devices to Not Auto-Run Content	Configure devices to not auto-run content from removable media.
Devices	Protect	9.4	Apply Host-Based Firewalls or Port-Filtering	Apply host-based firewalls or port-filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.
Data	Protect	10.1	Ensure Regular Automated BackUps	Ensure that all system data is automatically backed up on a regular basis.
Data	Protect	10.2	Perform Complete System Backups	Ensure that all of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.
Data	Protect	10.4	Protect Backups	Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.
Data	Protect	10.5	Ensure All Backups Have at Least One Offline Backup Destination	Ensure that all backups have at least one offline (i.e., not accessible via a network connection) backup destination.

Asset Type	Security Function	CIS #	Title	
Network	Protect	11.4	Install the Latest Stable Version of Any Security-Related Updates on All Network Devices	Install the latest stable version of any security-related updates on all network devices.
Network	Identify	12.1	Maintain an Inventory of Network Boundaries	Maintain an up-to-date inventory of all of the organization's network boundaries.
Network	Protect	12.4	Deny Communication Over Unauthorized Ports	Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.
Data	Identify	13.1	Maintain an Inventory of Sensitive Information	Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located on-site or at a remote service provider.
Data	Protect	13.2	Remove Sensitive Data or Systems Not Regularly Accessed by Organization	Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand-alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.
Data	Protect	13.6	Encrypt Mobile Device Data	Utilize approved cryptographic mechanisms to protect enterprise data stored on all mobile devices.

Asset Type	Security Function	CIS #	Title	
Data	Protect	14.6	Protect Information Through Access Control Lists	Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.
Network	Protect	15.7	Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data	Leverage the Advanced Encryption Standard (AES) to encrypt wireless data in transit.
Network	Protect	15.10	Create Separate Wireless Network for Personal and Untrusted Devices	Create a separate wireless network for personal or untrusted devices. Enterprise access from this network should be treated as untrusted and filtered and audited accordingly.
Users	Respond	16.8	Disable Any Unassociated Accounts	Disable any account that cannot be associated with a business process or business owner.
Users	Respond	16.9	Disable Dormant Accounts	Automatically disable dormant accounts after a set period of inactivity.
Users	Protect	16.11	Lock Workstation Sessions After Inactivity	Automatically lock workstation sessions after a standard period of inactivity.
N/A	N/A	17.3	Implement a Security Awareness Program	Create a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization. The organization's security awareness program should be communicated in a continuous and engaging manner.

Asset Type	Security Function	CIS #	Title	
N/A	N/A	17.5	Train Workforce on Secure Authentication	Train workforce members on the importance of enabling and utilizing secure authentication.
N/A	N/A	17.6	Train Workforce on Identifying Social Engineering Attacks	Train the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams, and impersonation calls.
N/A	N/A	17.7	Train Workforce on Sensitive Data Handling	Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive information.
N/A	N/A	17.8	Train Workforce on Causes of Unintentional Data Exposure	Train workforce members to be aware of causes for unintentional data exposures, such as losing their mobile devices or emailing the wrong person due to autocomplete in email.
N/A	N/A	17.9	Train Workforce Members on Identifying and Reporting Incidents	Train workforce members to be able to identify the most common indicators of an incident and be able to report such an incident.
N/A	N/A	19.1	Document Incident Response Procedures	Ensure that there are written incident response plans that define roles of personnel as well as phases of incident handling/management.
N/A	N/A	19.3	Designate Management Personnel to Support Incident Handling	Designate management personnel, as well as backups, who will support the incident handling process by acting in key decision-making roles.
N/A	N/A	19.5	Maintain Contact Information For Reporting Security Incidents	Assemble and maintain information on third-party contact information to be used to report a security incident, such as Law Enforcement, relevant government departments, vendors, and Information Sharing and Analysis Center (ISAC) partners.

Asset Type	Security Function	CIS #	Title	
N/A	N/A	19.6	Publish Information Regarding Reporting Computer Anomalies and Incidents	Publish information for all workforce members, regarding reporting computer anomalies and incidents, to the incident handling team. Such information should be included in routine employee awareness activities.

CSRIC notes that CIS does not provide the only set of recognized controls and does not endorse this method above and beyond any other recognized set of controls. However, CSRIC recommends implementing controls of this type, and advises that controls at or comparable to CIS IG1 can be implemented without significant cost by all organizations within the 9-1-1 community regardless of sophistication or resource availability. For those choosing a different method, US Department of Defense Cybersecurity Maturity Model Certification (CMMC)model provides a mapping of most of the industry-recognized cybersecurity controls against CMMC's controls, which can in turn be referenced to map control sets other than CMMC against each other.[44]

5.2.4 Findings Surrounding Best Practices

The matrix in Appendix A - Proposed Best Practices summarizes the findings associated with the Best Practice analysis provided by WG 4.

5.3 Recommendations

5.3.1 The following CSRIC recommendations are targeted to the Public Safety community:

- Public Safety entities should consider implementing cybersecurity service delivery models such as described in Appendix B - Cybersecurity Service Delivery Models.
- CSRIC recommends that spending on cybersecurity improvements be explicitly authorized as an eligible use of 9-1-1 funds. This recommendation applies to any national, state, or local laws, as well as any applicable regulations or policies that define eligible use of 9-1-1 funds.
- All organizations in the public safety service delivery chain shall have a documented cyber response plan, even if their operations are relatively basic and their associated response plan is also relatively basic. Organizations without in-house cybersecurity expertise should retain the services of an expert to assist in drafting their plans. Section 5.2.2.5 of this report shows that, on a purely statistical basis, it is a reasonable expense to

[44] See Office of the Under Secretary of Defense for Acquisition & Sustainment, Cybersecurity Maturity Model Certification (CMMC), CMMC Appendices, Appendix A. Retrieved 30 November 2020 at https://www.acq.osd.mil/cmmc/docs/CMMC_Appendices_V1.02_20200318.pdf.

develop a cyber response plan. This is above and beyond intangible costs, such as pain and suffering, which are caused by any 9-1-1 interruption.

- Public Safety is strongly encouraged to review funding allocation decisions to ensure that cybersecurity investments keep pace with technology innovations. This includes engaging the services of industry experts to assist in planning organizational approaches to addressing the cyber threat issue, and to assist in recommending budget changes that may be required to support your efforts to protect NG911 operations.
- PSAPs / ECCs should proactively work with a cyber-insurance provider to identify vendors that they want use for their cybersecurity implementation and ensure that the cyber-insurance company approves of the chosen vendor(s), i.e., that the vendors chosen are on the list of preferred vendors maintained by the organization's cybersecurity insurance provider.

  PSAPs/ECCs should consider the use of affirmative cyber-insurance language because the source of attack could be considered an exclusion to coverage. An example of a possible exclusion would be Acts of War which could be interpreted to excludes state actors. Care should be taken to ensure the policy language will include coverage for attacks from such sources. For example, the use of simple wording, affirmative coverage, and, ideally, eliminating some war and terrorism exclusions are all eminently positive ways for making sure that the PSAP/ECC that is impacted by a cyber-attack or a major breach is getting what it thinks it's buying: help when it needs it, paid quickly without a lot of argument.

- CSRIC recommends that PSAPs & ECCs ensure that all data coming into their centers outside of the regular emergency call path should meet the same security recommendations and standards as apply to other incoming emergency data, and should be limited to necessary communications only, controlled by security policies and tightly locked down to access only to the necessary system devices. Such terminations should meet at least the same access policies as to type of access (protocols) and password controls, as well as at least the same level of multifactor authentications as other incoming emergency data.

- CSRIC recommends that PSAPs/ECCs ensure that IoT smart cities devices and other IoT enabled devices are isolated from 9-1-1 networks.

- CSRIC VII recommends public safety personnel responsible for cybersecurity employ methodologies like the Factor Analysis of Information Risk (FAIR) Model to quantify their cyber-risk profile and corresponding mitigation and remediation strategies.

5.3.1.1 Recommendations Surrounding Prioritized Mitigation Solutions

- CSRIC recommends that public safety entities implement CIS Implementation Group 1 (IG1) controls or controls comparable to CIS IG1 across their organization. These controls can be implemented without significant cost by all organizations within the 9-1-1 community regardless of sophistication or resource availability and should be

prioritized for this reason. For those choosing a method other than CIS controls, the US DOD CMMC model provides a mapping of most of the industry-recognized cybersecurity controls against CMMC's controls, which can in turn be referenced to map control sets other than CMMC against each other.[45]

5.3.2 The following CSRIC recommendations are targeted to the Commission:

- CSRIC recommends the Commission foster and facilitate the development of a written consensus-driven model cyber response plan that can be used by all 9-1-1 organizations. This plan development and maintenance shall be sponsored by a reputable entity such as a government organization (such as the US 9-1-1 program or SAFECOM), a government advisory panel (such as CSRIC), and / or by a professional association. This model cyber response plan shall be developed with the input of industry experts, including 9-1-1 domain experts as well as general cyber security experts that may not have specific domain knowledge in 9-1-1. CSRIC notes that the creation of a model cyber response plan for 9-1-1 organizations could substantially reduce the amount of effort required to develop such a plan by each individual entity required to have a plan per our earlier recommendation along these lines. If a suitable template or set of templates can be used to develop a cyber response plan, the overall labor commitment could be reduced to one-half or less.
- CSRIC recommends that the Commission urge all organizations to implement a level of cyber controls equivalent or similar to the CIS IG1 set of controls regardless of size, capabilities, or resources.
- The Commission should encourage industry consideration of a call authentication mechanism for 9-1-1 calls in a legacy or transitional environment. Such a mechanism would allow a PSAP call taker to better assess the degree to which the information provided with a 9-1-1 call can be trusted.
- The Commission should consider having the Emergency Communications Cybersecurity Center (EC3) cost assessments shown in the TFOPA Report updated, as well as adding estimated costs for cyber training and cyber assessment.
- CSRIC recommends that the FCC attempt to foster communication with cybersecurity entities (e.g., ISO, CIS, NIST, NASCIO, etc.), to encourage them to adopt NG9-1-1 specific Best Practices that are fundamentally important to the security and reliability of Public Safety agencies throughout the country. This fostering could begin by including such entities in future CSRIC development work, especially as it applies to NG9-1-1 related Best Practices.
- CSRIC recommends that the Commission collect data from the 9-1-1 community about individual and organizational cybersecurity maturity, and consider referencing one or

[45] See Office of the Under Secretary of Defense for Acquisition & Sustainment, Cybersecurity Maturity Model Certification (CMMC), CMMC Appendices, Appendix A. Retrieved 30 November 2020 at https://www.acq.osd.mil/cmmc/docs/CMMC_Appendices_V1.02_20200318.pdf.

more security control models which include the maturity states and maps to the NIST framework when it evaluates overall NG9-1-1 maturity in its annual reports on NG9-1-1 readiness.[46]

- CSRIC encourages the FCC to support spending of 9-1-1 fees on cybersecurity as a matter of public policy.

5.3.2.1 Working Group 4 also provides recommendations to the Commission for future initiatives:

As stated in Report #2, CSRIC continues to support the need for future research into these topics.

- Over-the-top network solutions, such as Text To 9-1-1 (including examination and consideration of TTY architectures),
- Delivery of Supplemental Data and use of handset-based applications for vulnerabilities and exposures to cyber threats,
- IoT as a target,
- Smart Cities,
- 5G,
- How to deal with encrypted data destined for the PSAP/ECC,
- Other cybersecurity topics as they become known.

[46] See https://www.nist.gov/cyberframework; retrieved 21 December 2020.

6 Acronyms and Abbreviations

Many of the following definitions are based on and/or are generally consistent with NENA's "Master Glossary of 9-1-1 Terminology."[47] Others reflect generally available descriptions found on the Internet.

Term	Description
Advanced Encryption Standard (AES)	The Advanced Encryption Standard (AES) is a symmetric block cipher chosen by the U.S. government to protect classified information. AES is implemented in software and hardware throughout the world to encrypt sensitive data. It is essential for government computer security, cybersecurity and electronic data protection. (https://searchsecurity.techtarget.com/)
APCO (Association of Public Safety Communications Officials)	The world's oldest and largest professional organization dedicated to the enhancement of public-safety communications. APCO International serves the professional needs of its 15,000 members worldwide by creating a platform for setting professional standards, addressing professional issues and providing education, products and services for people who manage, operate, maintain, and supply the communications systems used by police, fire, and emergency medical dispatch agencies throughout the world.
BCF (Border Control Function)	Provides a secure entry into the ESInet for emergency calls presented to the network. The BCF incorporates firewall, admission control, and may include anchoring of session and media as well as other security mechanisms to prevent deliberate or malicious attacks on PSAPs or other entities connected to the ESInet.
Bring Your Own Device (BYOD)	BYOD stands for bring your own device. It's an IT policy that allows, and sometimes encourages, employees to access enterprise data and systems using personal mobile devices such as smartphones, tablets and laptops. (https://www.ibm.com/)
CIA (Confidentiality, Integrity and Availability)	Otherwise known as the CIA Triad, together, these three principles form the cornerstone of any organization's security infrastructure; in fact, they (should) function as goals and objectives for every security program.
CISA (Cybersecurity and Infrastructure Security Agency)	The Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future. CISA builds the national capacity to defend against cyber attacks and works with the federal government to provide cybersecurity tools, incident response services and assessment capabilities to safeguard the '.gov' networks that support the essential operations of partner departments and agencies.

[47] "NENA Master Glossary of 9-1-1 Terminology," National Emergency Number Association (NENA), revised January 2020. See: https://www.nena.org/page/Glossary

Term	Description
CMMC (Cybersecurity Maturity Model Certification)	A unifying standard for the implementation of cybersecurity across the Defense Industrial Base (DIB). The CMMC framework includes a comprehensive and scalable certification element to verify the implementation of processes and practices associated with the achievement of a cybersecurity maturity level. CMMC is designed to provide increased assurance to the Department that a DIB company can adequately protect sensitive unclassified information, accounting for information flow down to subcontractors in a multi-tier supply chain.
Criminal Justice Information Services (CJIS)	The FBI's Criminal Justice Information Services Division, or CJIS, is a high-tech hub in the hills of West Virginia that provides a range of state of-the-art tools and services to law enforcement, national security and intelligence community partners, and the general public.
CSF (Cybersecurity Framework)	A voluntary framework developed by NIST working with various stakeholders to identify existing standards, guidelines and practices that could be integrated into a guiding framework for reducing cyber risks to critical infrastructure.
CSRIC (Communications Security, Reliability, and Interoperability Council)	CSRIC's mission is to provide recommendations to the FCC to ensure, among other things, optimal security and reliability of communications systems, including telecommunications, media, and public safety.
DDOS (Distributed Denial of Service)	The attack source is more than one, often thousands of unique IP addresses. A DDoS attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for example a botnet) flooding the targeted system with traffic.
DNS (Domain Name Service)	A globally distributed database for the resolution of host names to numeric IP addresses.
EC3 (Emergency Communications Cybersecurity Center)	The federal interagency focal point for interoperable and operable communications coordination. Its members represent the federal government's broad role in emergency communications, including regulation, policy, operations, grants, and technical assistance.
ECC (Emergency Communications Centers)	A facility that is designated to receive requests for emergency assistance, including but not limited to 9-1-1 calls, and staffed to perform one or more of the following functions: • Determine the location where an emergency response is being requested. • Interrogate callers to identify, assess, prioritize, and classify requests for emergency assistance and other gathered information. • Determine the appropriate emergency response required. • Assess the available emergency response resources that are, or will be, available in the time required. • Dispatch appropriate emergency response providers. • Transfer or exchange requests for emergency assistance and other gathered information with other emergency communications centers and emergency response providers. • Analyze and respond to communications received from emergency response providers and coordinate appropriate actions. • • Support incident command functions.

Term	Description
Emergency Services IP Network (ESInet)	A managed IP network that is used for emergency services communications, and which can be shared by all public safety agencies. It provides the IP transport infrastructure upon which independent application platforms and core services can be deployed, including, but not restricted to, those necessary for providing NG9-1-1 services. ESInets may be constructed from a mix of dedicated and shared facilities. ESInets may be interconnected at local, regional, state, federal, national and international levels to form an IP-based inter-network (network of networks). The term ESInet designates the network, not the services that ride on the network. https://nenawiki.org/wiki/Main_Page
MS-ISAC (Multi-State Information Sharing and Analysis Center)	A division of the Center for Internet Security, MS-ISAC is the focal point for cyber threat prevention, protection, response and recovery for the nation's state, local territory and tribal (SLTT) governments.
NENA (The 9-1-1 Association)	NENA serves the public safety community as the only professional organization solely focused on 9-1-1 policy, technology, operations, and education issues. With more than 12,000 members in 48 chapters across North America and around the globe, NENA promotes the implementation and awareness of 9-1-1 and international three-digit emergency communications systems. See http://www.nena.org/page/aboutfaq2017 for more details.
NIST (National Institute of Standards and Technology)	A part of the United States Department of Commerce that oversees the operation of the U.S. National Bureau of Standards. NIST works with industry and government to advance measurement science and to develop standards in support of industry, commerce, scientific institutions, and all branches of government. Their mission is to promote innovation and industrial competitiveness. https://www.nist.gov/
Phishing	Phishing is the fraudulent attempt to obtain sensitive information or data, such as usernames, passwords and credit card details, by disguising oneself as a trustworthy entity in an electronic communication. Typically carried out by email spoofing, instant messaging, and text messaging, phishing often directs users to enter personal information at a fake website which matches the look and feel of the legitimate site. Phishing is an example of social engineering techniques used to deceive users. Users are lured by communications purporting to be from trusted parties such as social web sites, auction sites, banks, colleagues/executives, online payment processors or IT administrators. https://en.wikipedia.org/wiki/Phishing
PSAP (Public Safety Answering Point)	An entity responsible for receiving 9-1-1 calls and processing those calls according to a specific operational policy. See the NENA Master Glossary for more details.
Security Operations Center (SOC)	A security operations center (SOC) is a command center facility for a team of information technology (IT) professionals with expertise in information security (infosec) who monitors, analyzes and protects an organization from cyber attacks. (https://searchsecurity.techtarget.com/)
SLTT (State, Local, Tribal and Territorial)	A term referring to four categories of governmental entities.

Term	Description
Swatting	Swatting is a form of harassment in which attackers try to trick police forces into sending a heavily armed strike force — often a SWAT team, which gives the technique its name — to a victim's home or business. www.csoonline.com
TCP (Transmission Control Protocol)	Transmission Control Protocol - highly reliable host-to-host protocol between hosts in a packet-switched computer communication networks, and in interconnected systems of such networks. (IETF 1981 https://tools.ietf.org/html/rfc793)
TDOS (Telephony Denial of Service)	Telephony Denial of Service - the attack relies on impersonation in order to obscure the origin of an attack that is intended to tie up telephone resources. (IETF 2014 https://tools.ietf.org/html/rfc7375)
TFOPA (Task Force on Optimal PSAP Architecture)	The FCC's Task Force on Optimal Public Safety Answering Point (PSAP) Architecture was directed to study and report findings and recommendations on structure and architecture in order to determine whether additional consolidation of PSAP infrastructure and architecture improvements would promote greater efficiency of operations, safety of life, and cost containment, while retaining needed integration with local first responder dispatch and support.
UDP (User Datagram Protocol)	A datagram mode of packet-switched computer communication in the environment of an interconnected set of computer networks. This protocol assumes that the Internet Protocol (IP) is used as the underlying protocol. (IETF 1980 https://tools.ietf.org/html/rfc768)
Universal Serial Bus (USB)	**Universal Serial Bus (USB)** is an industry standard that establishes specifications for cables and connectors and protocols for connection, communication and power supply (interfacing) between computers, peripherals and other computers.[3] A broad variety of USB hardware exists, including eleven different connectors, of which USB-C is the most recent. (https://en.wikipedia.org/)
US-CERT (United States Computer Emergency Readiness Team)	Information technology (IT) security organization. The purpose of CERT is to respond to computer security incidents, report on vulnerabilities and promote effective IT security practices throughout the country. https://www.us-cert.gov/

Appendix A - Proposed Best Practices

Based on an evaluation of existing Best Practices that addressed cybersecurity considerations, and an analysis of the use cases and security controls described in Report 2, *CSRIC Report on Security Risks and Best Practices for Mitigation in 9-1-1 in Legacy, Transitional, and NG9-1-1 Implementations*, the WG identified gaps in existing Best Practices and developed proposals for new best practices focusing on the identification and mitigation of cybersecurity risks in legacy E9-1-1 and transitional and end-state NG9-1-1 environments. This Appendix describes proposals for modified and new Best Practices and the applicability of these Best Practices to legacy E9-1-1, transitional and end-state NG9-1-1 implementations. Consistent with Report 2, this Appendix applies the following definitions to the terms "Legacy", "Transition" and "End State" as used in the tables below:

- *"Legacy"* refers to a state in which 9-1-1 services are provided by the traditional incumbent local exchange carrier (ILEC) with circuit-switched infrastructure and Automatic Location Identification (ALI) circuits.
- *"Transitional"* refers to a state in which services have begun the migration from the legacy environment to an IP-enabled infrastructure. During a Transitional State, the Emergency Services IP Network (ESInet) is in place supported by the associated Next Generation 9-1-1 Core Services, but the originating networks and PSAPs that interconnect with the ESInet and associated NG9-1-1 Core Services may or may not have evolved to support NG9-1-1 functionality and interfaces.
- *"End State"* refers to the state in which PSAPs have evolved to become ECCs and are served by standards-based NG9-1-1 systems and/or elements and Originating Service Providers (OSPs) are providing SIP interfaces with location information during call setup, and ESInets are interconnected providing interoperability on a national basis, supported by established agreements, policies and procedures.

Table A includes existing Best Practices, some of which were modified based upon the analysis of the Working Group. The final recommended text is shown in this table.

Table A

BP #	Table A: EXISTING Best Practice	Legacy	Transition	End State
12-12-0779	Network Operators, Service Providers, Equipment Suppliers and Public Safety should establish a means to allow for coordination between cyber and physical security teams supporting preparedness, response, investigation and analysis.	TRUE	TRUE	TRUE
12-12-3269	Network Operators, Service Providers and Public Safety should establish policies governing data, metadata, and other media that hold information that could be used to compromise the security in an NG9-1-1 system.		TRUE	TRUE
12-12-3270	Network Operators, Service Providers and Public Safety should establish and enforce policies for log in requirements, password protection, screenlock upon activity timeout, and other physical security measures to prevent visitors and outside contractors from accessing NG 9-1-1 systems.	TRUE	TRUE	TRUE
12-12-3273	Network Operators, Service Providers and Public Safety should establish and enforce policies that ensure cloud based Next Gen 9-1-1 services provide resilience, performance and security that meet established best practices for public safety and 9-1-1 and that leverage the scalable and enhanced information technology capacities of cloud based Next Gen 9-1-1 services.		TRUE	TRUE

BP #	Table A: EXISTING Best Practice	Legacy	Transition	End State
12-12-3274	Network Operators, Service Providers should use strong certificate-based authentication ensuring network access, digital content and software services can be secured from unauthorized access. This applies to Public Safety only in an NG9-1-1 environment.		TRUE	TRUE
12-12-3275	Network Operators, Service Providers, Equipment Suppliers and Public Safety should support Border Control Functions (BCFs) that provide border firewall functionality including application and network layer protection and scanning, resource and admission control, and Denial of Service (DoS) detection and protection, as well as Session Border Control (SBC) functionality including: identification of emergency call/session and priority handling for the IP flows of emergency call/session traffic; conformance checking and mapping (if applicable) of priority marking based on policy for emergency calls/sessions; SIP protocol normalization; Network Address Translation (NAT) and Network Address and Port Translation (NAPT) Traversal; IPv4/IPv6 Interworking; Signaling Transport Protocol Support; and QoS/Priority Packet Marking.		TRUE	TRUE
12-12-3290	Network Operators and Service Providers should apply caller authentication/verification techniques (e.g., using the SHAKEN framework) to mitigate Caller ID spoofing in general, including on incoming 9-1-1 calls, call backs and administrative emergency lines.		TRUE	TRUE
12-12-3291	Network Operators, Service Providers and Public Safety should coordinate DOS and TDOS detection, verification and recovery efforts with local law enforcement, cybersecurity task forces, State Threat Assessment centers and other law enforcement agencies. The PSAP should have procedures in place that minimize the impact of DOS and TDOS while preserving the evidence needed to support the investigation.	TRUE	TRUE	TRUE
12-12-8118	Network Operators, Service Providers and Public Safety should provide DNS DDoS protection by implementing protection techniques such as: 1) Rate limiting DNS network connections 2) Provide robust DNS capacity in excess of maximum network connection traffic 3) Have traffic anomaly detection and response capability 4) Provide secondary DNS for back-up 5) Deploy Intrusion Prevention System in front of DNS to provide near real time alerts of a cyber-attack to provide near real time alerts of a cyber-attack. 6) Use cloud technologies to enable rapid instantiation of alternate networks and DNS capabilities. This BP applies to Public Safety only in an NG9-1-1 environment.		TRUE	TRUE
12-12-8517	Network Operators, Service Providers, Equipment Suppliers and Public Safety should review audit trails if information has been leaked or the release policy has not been followed. Change passwords, review permissions, and perform forensics as needed. Inform others at potential risk for similar exposure, and include security responsibilities in performance improvement programs that may include security awareness refresher training.	TRUE	TRUE	TRUE

BP #	Table A: EXISTING Best Practice	Legacy	Transition	End State
12-12-8527	Network Operators, Service Providers and Public Safety should prepare a disaster recovery plan to implement upon DNS server compromise. The plan should incorporate procedures to, first flush the DNS cache and, failing that, implement elements that may include but are not limited to: 1) bring-on additional hot or cold spare capacity, 2) bring up a known good DNS server from scratch on different hardware, 3) Reload and reboot machine to a known good DNS server software (from bootable CD or spare hard drive), 4) Reload name resolution records from a trusted back-up. After the DNS is again working, conduct a post-mortem of the attack/response. This applies to Public Safety only in an NG9-1-1 environment.		TRUE	TRUE
12-12-8528	Network Operators, Service Providers and Public Safety should consider one or more of the following steps if the DNS server is under attack, 1) Implement reactive filtering to discard identified attack traffic, if possible, 2) Rate-limiting traffic to the DNS server complex, 3) Deploy suitable Intrusion Prevention System in front of DNS servers, 4) Deploy additional DNS server capacity in a round-robin architecture, 5) Utilize DoS/DDoS tracking methods to identify the source(s) of the attack, or 6) Move name resolution service to a third party provider. This applies to Public Safety only in an NG9-1-1 environment.		TRUE	TRUE
12-12-8540	Network Operators, Service Providers and Public Safety should consider terminating all current remote access, limiting access to the system console, or other tightened security access methods, when an unauthorized remote access to an OAM&P system occurs. Continue recovery by re-establishing new passwords, reloading software, running change detection software, or other methods, continuing quarantine until recovery is validated, as practical.	TRUE	TRUE	TRUE
12-12-8561	Network Operators, Service Providers and Public Safety, should when a network element or server is under DoS attacks, evaluate the network and ensure the issue is not related to a configuration/hardware issue. If it is not a configuration/hardware issue, determine direction of traffic and work with distant end to stop inbound traffic. Consider adding more local capacity (bandwidth or servers) to the attacked service. Where available, deploy DoS/DDoS specific mitigation devices and/or use anti-DoS capabilities in local hardware. Coordinate with HW vendors for guidance on optimal device configuration. Where possible, capture hostile code and make available to organizations such as US-CERT and NCS/NCC for review. This BP applies to Public Safety only in an NG9-1-1 environment.		TRUE	TRUE
12-12-8758	Network Operators, Service Providers and Public Safety should establish policies, and procedures to support early recognition and isolation of potential bad actors to minimize impact to the network. This applies to Public Safety only in an NG9-1-1 environment.		TRUE	TRUE

BP #	Table A: EXISTING Best Practice	Legacy	Transition	End State
12-12-8929	Network Operators, Service Providers and Public Safety should employ authentication, authorization, accountability, integrity, and confidentiality mechanisms (e.g., digital signature and encrypted VPN tunneling), when they employ the Public Internet for signaling, transport, or maintenance communications and any maintenance access to Network Elements.	TRUE	TRUE	TRUE
12-12-8933	Network Operators, Public Safety should establish login and access controls that establish accountability for changes to node translations and configuration.	TRUE	TRUE	TRUE
12-8-8533	Network Operators, Service Providers should if an SS7 Denial of Service (DoS) attack is detected, more aggressively apply the same thresholding and filtering mechanism used to prevent an attack (NRIC BP 8053). The alert/alarm will specify the target of the attack. Isolate, contain, and, if possible, physically disconnect the attacker. If necessary, isolate the targeted network element and disconnect to force a traffic reroute.	TRUE	TRUE	
BP: 12-8-8768	Network Operators, Service Providers, Equipment Suppliers, and Public Safety should support multi-factor authentication to increase confidence in the identity of an entity. 12-10-2020: Add the explanation verbiage shown here to the Note field instead. Multi-factor authentication involves validating the authenticity of the identity of an entity by verifying multiple identifiers and attributes associated with the entity. The data for multi-factor authentication capabilities should be organized based something you are (e.g., physical of behavioral characteristics of an end user or customer's characteristic or attribute that is being compared such as typing patterns, voice recognition), something you have (e.g., a driver's license, or a security token) and something you know (e.g., a password, pin number, security image).		TRUE	TRUE

Table B

BP #	Table B: PROPOSED NEW Best Practices	Legacy	Transition	End State
1.	Network Operators, Service Providers and Public Safety should ensure that any 9-1-1 cyber architecture plan addresses a reliable fail-over capability that includes elements of physical and logical diversity, redundancy, and resiliency.	TRUE	TRUE	TRUE
2.	Public Safety should provide common cyber practices for all interconnection paths, which may come from multiple service providers for resiliency sake.	TRUE	TRUE	TRUE

BP #	Table B: PROPOSED NEW Best Practices	Legacy	Transition	End State
3.	Public Safety should provide common cyber practices for all interconnection paths that support mutual aid/inter-local arrangements for overflow and failover to other ECCs.	TRUE	TRUE	TRUE
4.	Network Operators and Public Safety should ensure that staff is well trained, in reporting of security incidents, weaknesses and suspicious activity and are equipped with intrusion detection capability, response tools, and processes linking operations alarms with security alerts that would support rapid response and mitigation capability.	TRUE	TRUE	TRUE
5.	Network Operators and Public Safety should Monitor information flow and follow cyber requirements on handling of sensitive data.	TRUE	TRUE	TRUE
6.	Network Operators and Public Safety should consider restricting recursion and disabling the ability to send additional delegation information to help prevent DNS-based DoS attacks and cache poisoning.			TRUE
7.	Network Operators and Public Safety should conduct a periodic review of US-CERT, and similar security sites for up-to-date cybersecurity prevention tips.	TRUE	TRUE	TRUE
8.	Network Operators should be prepared to initiate alternate treatment of 9-1-1 calls that meet specific criteria when requested to do so by Public Safety agencies that are experiencing a TDoS or other type of attack.	TRUE	TRUE	TRUE
9.	Public Safety should ensure that they have access to the phone number and direct contact information for the network operator's personnel or division that is equipped to respond to Public Safety TDoS attacks.	TRUE	TRUE	TRUE
10.	Public Safety should log all available information associated with calls that are associated with a DDoS or TDoS attack and share that information with emergency communications centers, other PSAPs/Public Safety Agencies, government IT departments, and any related government agency with a vested interest in emergency communications continuity of operation.	TRUE	TRUE	TRUE
11.	Public Safety should support configuration changes to isolate critical phone lines (incoming 9-1-1 calls for service) from administrative and other lines, taking into account hunt-groups, busy or no-answer rollover to other lines, rollover to other PSAPs, etc. to prevent an overload of non-critical lines from rolling-over to lines answered by 9-1-1 call-takers when experiencing a TDoS attack.	TRUE	TRUE	TRUE
12.	Public Safety should limit the amount and type of information about the ECC is shared publicly, e.g., administrative telephone numbers, number of staff, type of communication technology in use, etc.	TRUE	TRUE	TRUE
13.	Public Safety should have a keen attention to detail by well-trained staff to recognize spoofed or non-valid information to mitigate the impacts of cyber-attacks on incoming 9-1-1 calls and calls received on administrative emergency lines.	TRUE	TRUE	TRUE
14.	Public Safety should have a well-designed mutual aid plan with neighboring agencies (PSAPs) to help mitigate a swatting attack.	TRUE	TRUE	TRUE

BP #	Table B: PROPOSED NEW Best Practices	Legacy	Transition	End State
15.	Network Operators, Service Providers and Public Safety should ensure laws or rules are in place along with service level agreements identifying requirements for service providers' cooperation in providing the location of cellular phones and other devices accessing 9-1-1 services to quickly assist with a swatting attack.	TRUE	TRUE	TRUE
16.	Public Safety should work with the originating service provider and/or text control center in a swatting attack to assist with identifying or locating the orchestrators.	TRUE	TRUE	TRUE
17.	Network Operators, Service Providers, and Public Safety should continuously monitor IP traffic for scanning, phishing attacks, and other suspicious cyber activity.		TRUE	TRUE
18.	Network Operators, Service Providers, and Public Safety should provide a well-architected, segmented network.	TRUE	TRUE	TRUE
19.	Public Safety and Equipment Suppliers should support effective end point security and use resilient end points that don't provide access to common tools typically used by hackers to encrypt files on an end point.			TRUE
20.	Public Safety should provide three (3) system back-ups on two (2) different forms of media storage (such as cloud, tape, external drive, flash drive) that can be connected on demand. Further, do not allow any of them to be connected until needed. One of the backups should be stored offsite, and geographically & logically separated from the others. Routine testing should be done to allow the ECC to restore hosts.	TRUE	TRUE	TRUE
21.	Network Operators and Public Safety should identify deleted logs by searching for instances of log deletion or last-seen log events.	TRUE	TRUE	TRUE
22.	Network Operators and Public Safety should ensure adequate logging and visibility on ingress and egress points.	TRUE	TRUE	TRUE
23.	Network Operators and Public Safety should search server file systems for unusual files or scripts.	TRUE	TRUE	TRUE
24.	Network Operators and Public Safety should detect malicious use of legitimate credentials.		TRUE	TRUE
25.	Public Safety should scan all emails, attachments, and downloads (both on the host and at the mail gateway) with a reputable anti-virus solution that includes cloud reputation services.	TRUE	TRUE	TRUE
26.	Public Safety should segment any critical networks or control systems from administrative systems and networks.	TRUE	TRUE	TRUE
27.	Public Safety should provide cyber hygiene training to staff that includes informing end users on proper email and web usage, highlighting current information and analysis, and including common indicators of phishing.	TRUE	TRUE	TRUE
28.	Public Safety should ensure that network administrators use non-privileged accounts for email and internet access.	TRUE	TRUE	TRUE
29.	Public Safety should periodically conduct searches of publicly available information to ensure no sensitive information has been disclosed.	TRUE	TRUE	TRUE
30.	Network Operators, Service Providers, Equipment Suppliers, and Public Safety should implement the "least-privilege-principle" for security in all public safety systems; meaning, provide access only to those resources that an individual should have access to.	TRUE	TRUE	TRUE
31.	Network Operators, Service Providers and Public Safety should log, monitor, and audit all employee electronic activity.		TRUE	TRUE

BP #	Table B: PROPOSED NEW Best Practices	Legacy	Transition	End State
32.	Network Operators, Service Providers, Equipment Suppliers, and Public Safety should exercise third-party vulnerability testing on a regular basis.	TRUE	TRUE	TRUE
33.	Network Operators, Service Providers, Equipment Suppliers, and Public Safety should maximize insider threat awareness among employees, including training about personal vulnerabilities, being engineered to become an insider threat, and detecting insider threats in their businesses.	TRUE	TRUE	TRUE
34.	Public Safety shall implement and follow a recognized cybersecurity controls framework that includes evaluating where they fall along a given method's maturity continuity, which cyber controls they have already implemented, and which are the highest priority to implement first.	TRUE	TRUE	TRUE
35.	Network Operators, Service Providers, and Public Safety should patch hosts as patches become available, on the system.	TRUE	TRUE	TRUE
36.	Public Safety should disallow emergency services work on untrusted personal devices unless there are defenses in place.	TRUE	TRUE	TRUE
37.	Public Safety should disallow personal use of official emergency services devices in untrusted networks (e.g., Starbucks), unless there are end point defenses in place.	TRUE	TRUE	TRUE

36
37

Appendix B - Cybersecurity Service Delivery Models

Working with the FCC, CISA, Department of Homeland Security-Science & Technology and a variety of stakeholders the WG has compiled a focused description and narrative of the Emergency Communications Cybersecurity Center (EC3) concept. The concept was originally proposed by the FCC's Task Force on Optimal PSAP Architecture (TFOPA). The full report can be found here: https://www.fcc.gov/about-fcc/advisory-committees/general/task-force-optimal-public-safety-answering-point

The EC3 will take on the role of providing Intrusion Detection and Prevention Systems (IDPS)services to ECCs and any other emergency communications service or system that would consider utilizing a centralized, core services-based architecture. This approach would allow public safety to build one infrastructure and use it for many clients. This provides significant economies of scale, puts multiple Federal, State, Local and Tribal resources into the same protection scheme, and allows for sharing of data, mitigation strategies, and recovery efforts across enterprise.

Based on research and input from these various sources, CSRIC VII believes it is important to consider this type of approach as part of a holistic cybersecurity program. What follows are high level observations that tie to recommendations found elsewhere in this report.

The high-level goals of EC3 should include:

- Building a network of partner organizations to share cybersecurity best practices and information (e.g., federal, state, local, tribal, and territorial [FSLTT] stakeholders, private-sector providers)
- Tailoring a scalable and customizable suite of cybersecurity services to remedy capability gaps in traditional cybersecurity solutions

To achieve these goals, two mission support and three system capabilities for EC3s are presented below (see Table 4). Mission support capabilities encourage a collaborative approach to cybersecurity that connects public safety communications stakeholders and fosters information sharing. System capabilities provide a menu of cybersecurity services that scale to meet ECC/PSAP's specific cybersecurity and NG911 architecture requirements.

Table 4: EC3 Capabilities

Capability	Description
Mission Support Capabilities	
Partner outreach	Collaborative organizational structure that facilitates engagement with other public safety communications stakeholders at all levels of government, as well as private-sector partners
Incident information sharing	Formalized agreements between EC3 participants to share cyber incident information, with the goal of informing response and recovery activities
System Capabilities	

Capability	Description
Intrusion detection and prevention systems (IDPS)	Collection of sensors which centralizes monitoring of all incoming data, alerting cybersecurity personnel to suspicious data and preventing unauthorized network access attempts
Telephony denial of service detection	System designed to detect potentially malicious incoming calls and act to preserve day-to-day voice answering capabilities
Security information and event management	Suite of software tools which gather and analyze network activity, including consolidating and correlating system logs

As ECCs/PSAPs adopt NG911, their operations are becoming increasingly interconnected via IP-based networks (e.g., ESInets, the Internet). Traditional cybersecurity solutions may not provide sufficient protection for NG911 services due to the unique requirements of public safety communications users. For example, a traditional cybersecurity solution may rely on a rules-based scheme to protect networks (e.g., if incoming data does not meet certain criteria, the network does not accept suspicious data). However, rejecting data for an ECC/PSAP may inadvertently decline legitimate request for assistance, necessitating cybersecurity solutions tailored for NG911 systems. EC3s can help ECCs/PSAPs bridge the gap between traditional cybersecurity solutions and NG911 requirements. Cybersecurity protections should incorporate safeguards for both communications and information technology (IT) systems, adapting solution sets to preserve public safety critical communications. As ECCs/PSAPs adopt NG911 capabilities, network administrators face increasing cyber risk from a variety of sources as described in **Table 5**.

Table 5: ECC/PSAP Cyber Threats and Hazards

Threat	Description
Distributed Denial of Service (DDoS) Attacks	Attacks designed to disrupt network operations through repeated and sustained requests for information, overloading network capacity and preventing normal operations
Telephony Denial of Service (TDoS) Attacks	Attacks designed to disrupt voice services through repeated and sustained phone calls, overloading call capacity and preventing valid users from connecting to ECCs/PSAPs
Malicious Software and Applications (i.e., Malware)	Software programs and applications that provide unauthorized access to networks, enabling malicious actors to potentially steal, corrupt, modify, or monitor data (e.g., first responder location information)
Phishing and Spear-Phishing	Targeted social engineering attacks, aimed at public safety users, designed to trick users into sharing credentials (e.g., usernames, passwords)
Man-in-the-Middle Attacks	Attacks designed to intercept data during transmission, allowing malicious actors to monitor, change, or disrupt information sent from one user to another

Threat	Description
Unauthorized Network and Data Access	Unauthorized access to network functions or data as a result of insufficient identity, credentialing, or access protections, such as a malicious actor using stolen credentials, allowing unauthorized devices to connect to networks, or the inadvertent disclosure of sensitive data (i.e., data leaks)
Insider Threats	Employee or other authorized personnel who leverage access to steal, corrupt, destroy, or otherwise use data in an unauthorized manner

EC3s support a collaborative, service-based approach to cybersecurity. EC3s should serve as a cybersecurity nexus, enabling ECCs/PSAPs to engage with FLSTT organizations and private-sector providers, as well as leverage relationships to share incident information with other public safety information sharing organizations (e.g., fusion centers). EC3s should incorporate two mission support capabilities, described in **Table 6**.

Table 6: EC3 Mission Support Capabilities

Capability	Description	Impact
Partner Outreach	Collaborative organizational structure that facilitates engagement with other public safety communications stakeholders at all levels of government, as well as private-sector partners	Empowers EC3 participants to share cybersecurity best practices and research on emerging threats, leverage resources for shared initiatives, and increase resiliency through mutual aid
Incident Information Sharing	Formalized agreements between EC3 participants to share cyber incident information, with the goal of informing response and recovery activities	Enhances situational awareness of ongoing cyber incidents, allowing partners to analyze threats and share technical data to improve future system resiliency

EC3s provide a scalable and customizable cybersecurity-as-a-service solution tailored for public safety communications stakeholders. EC3 should provide ECCs/PSAPs with the flexibility to select from a menu of services that meet their specific cybersecurity and NG9-1-1 architecture requirements. An EC3's suite of services should scale to protect individual ECCs/PSAPs, state-wide ESInets, or regional ESInets, depending on the needs of FSLTT partners. A host-based solution would enable EC3s to offer layered security with centralized monitoring and analysis capabilities. EC3s should incorporate three core services (see **Table 7**) to address the most common cyberattack vectors.

Table 7: EC3 System Capabilities

Capability	Description	Impact
Intrusion Detection and Prevention System (IDPS)	Collection of sensors which centralizes monitoring of all incoming data, alerting cybersecurity personnel to suspicious data and preventing unauthorized network access attempts	Enables real-time monitoring and visualization of all incoming data, standardizes reporting to exclude personally identifiable information, and allows ECC/PSAPs to automatically share data with the EC3 and other trusted partners
TDoS Detection	System designed to detect potentially malicious incoming calls and act to preserve day-to-day voice answering capabilities	Preserves ECC/PSAP ability receive and send critical voice data
Security Information and Event Management (SIEM)	Suite of software tools which gather and analyze network activity, including consolidating and correlating system logs	Provides a customizable situational awareness solution, enabling EC3 staff to view network configurations, escalate data for analysis, collect incident information, and analyze network vulnerabilities post-incident

EC3s provide a suite of supplemental cybersecurity services, addressing specific capability gaps unique to public safety communications stakeholders. ECCs/PSAPs should already employ strong general cybersecurity best practices, such as those detailed in the National Institute of Standards and Technology (NIST) Cybersecurity Framework, to protect networks against common cybersecurity threats.[48] Public safety communication requirements and cyberthreats are constantly evolving. In the future, EC3's suite of services may expand to incorporate additional cybersecurity detection, mitigation, and information sharing technologies.

To achieve success, EC3 strategic planning will rely on a variety of FLSTT stakeholders working together. Technical- and user-requirement working groups, pilot participants, and additional stakeholders may be necessary to facilitate concept development and implementation activities.

Process considerations identify the operational and system factors that inform EC3 implementation. EC3's process considerations include training, IT, and resiliency requirements. The process considerations in this document are representative and not comprehensive.

EC3 partners should identify cybersecurity staff qualifications and training requirements. EC3's mission requires both cybersecurity and public safety communications expertise. EC3 partners should consider adapting existing cybersecurity qualification resources to public safety communications needs (e.g., NIST National Initiative for Cybersecurity Education

[48] NIST (2016). Framework for Improving Critical Infrastructure Cybersecurity https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Cybersecurity Workforce Framework).[49] Developing an EC3 specific qualification guide helps maintain a minimum level of cybersecurity capabilities across the EC3 network. In addition, EC3 partners may tailor future training requirements to meet public safety technology advances and emerging cybersecurity threats.

EC3 capabilities require a minimum level of IT infrastructure, including modern computing equipment, connections to information sharing tools, and the ability to access cloud-based cybersecurity resources. IT infrastructure should support up-to-date software (e.g., operating systems), external network connections (e.g., the Internet), secure database access, email, and telephone capabilities. EC3s partners should consider leveraging existing networking infrastructure to reduce overhead costs, such as co-locating at existing network operations facilities (e.g., SLTT cyber network operation centers, ESInet regional nodes, Fusion Centers). EC3 partners should use information sharing tools to exchange cyber incident and system configuration data, analyze threats, update threat databases, and inform response and recovery actions. Information sharing capabilities should include access to interagency systems, such as the Homeland Security Information Network, and unclassified systems for cyber incident and threat information.

EC3s facilities should support ECC/PSAP continuous IT, call answering, and cybersecurity operations (i.e., 24 hours a day, 7 days a week). EC3 infrastructure should incorporate resiliency features, such as back-up network connections, onsite emergency power, and secured access points. EC3 facilities should identify critical infrastructure dependences and develop response and recovery plans as appropriate. As the EC3 concept matures, EC3 facilities should regularly assess infrastructure vulnerabilities and harden systems to close gaps. EC3 partners should also integrate into ECC/PSAP continuity of operations planning, clearly defining EC3's role and responsibilities for maintaining continuous service (e.g., initiating call overflow to maintain voice capabilities). Resiliency requirements will vary considerably from location-to-location, depending on local threats and hazards.

It is important to note that bearing in mind financial, operational, and technical constraints faced by the majority of ECCs has been taken into account when creating this design and concept. Rather than requiring ECCs to build and staff such facilities, the EC3 concept allows for ECCs from within and across jurisdictions, to interconnect to the core cybersecurity system and benefit from its capabilities, whether state, local, tribal, or territorial. This is also intended to provide a scalable, and customizable, approach. This means for localities with larger than average emergency communications systems (major metropolitan areas such as New York, Los Angeles, etc.) there is ample opportunity to construct a single EC3 to serve this individual customer. However, any EC3 should be designed and constructed in such a way that it will interconnect with other EC3's throughout the United States with the same functions and requirements. From the regional or State level, the information should flow to centralized repositories with adequate service capabilities to support multiple clients, and incidents, in real time.

[49] NIST National Initiative for Cybersecurity Education (2017). Cybersecurity Workforce Framework, see: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

The EC3 represents an enterprise level approach to cybersecurity that is very much needed as emergency communications progresses to an IP based, more robust, more comprehensive system. As seen with responder focused systems that provide interoperable, interactive, real-time communications, information flow is becoming broader and more data intensive. As this shift occurs, the threat to the networks and systems that support the data flow also increases. The EC3 as proposed would become part of a more comprehensive and cooperative approach to defending these networks and systems to the benefit of users, and citizens, alike.

DHS Developed Scenarios

- The scenarios outlined below highlight how EC3s might support ECC/PSAP partners during real-world cybersecurity incidents, specifically detecting TDoS and mitigating malware threats. The sections below outline the scenario and steps to address each incident. capabilities.

Table 8 and **Table 9** highlight EC3's role, capabilities, and solutions during each step.

Telephony Denial of Service Mitigation

Scenario: A TDoS incident generates a large volume of 911 calls and texts to an ECC/PSAP. EC3 supports ECC/PSAP partners by:

- Baselining call volume for day-to-day operations
- Validating incoming call information
- Managing call volume to maintain call answering capabilities.

Table 8: TDoS Detection Roles, Capabilities, and Solutions

Step	EC3 Role	Capabilities Required	Solutions
Call Volume Baseline Assessment	Determine the typical call volume associated with day-to-day ECC/PSAP operations and identify anomalous activity patterns	Sensors monitoring ESInet traffic Analytics and detection tools processing multiple sources of real-time data	IDPS SIEM
Call Validation	Assess the legitimacy of incoming communications (e.g., check for spoofed phone numbers) and either 1) forward traffic for action or 2) flag suspicious traffic for analysis and separate from day-to-day call answering	Sensors monitoring ESInet traffic Analytics and detection tools processing multiple sources of real-time data Shared situational awareness and information sharing environment with other EC3 partners Formal incident response and recovery procedures involving other EC3s, FSLTT partners, and private-sector providers Event analysis escalation to cybersecurity subject matter experts	Partner Outreach Incident Information Sharing IDPS SIEM TDoS Detection

Step	EC3 Role	Capabilities Required	Solutions
Call Volume Management	Measure call volume, compare against a baseline of day-to-day operations, and maintain call answering capabilities (e.g., requesting support from mutual aid partners, activating call overflow capacity).	Sensors monitoring ESInet traffic Analytics and detection tools processing multiple sources of real-time data Shared situational awareness and information sharing environment with other EC3 partners Formal incident response and recovery procedures involving other EC3s, FSLTT partners, and private-sector providers Resiliency measures to maintain call answering capabilities (e.g., call overflow capacity, mutual aid with other ECC/PSAPs)	Partner Outreach Incident Information Sharing IDPS TDoS Detection SIEM

Malware Mitigation

Scenario: An unknown third-party uses multimedia data (e.g., pictures, video) to introduce malware onto an ESInet, severely disrupting operations. EC3 supports ECC/PSAP partners by:

- Assessing incoming multimedia content for anomalies
- Detecting and reporting incident
- Supporting response and recovery operations

Table 9: Malware Mitigation Roles, Capabilities, and Solutions

Step	EC3 Role	Capabilities Required	Solutions
Incoming Content Assessment	Analyze incoming incident data and multimedia content (e.g., pictures, video) and flag suspicious information for analysis	Sensors monitoring ESInet traffic Analytics and detection tools processing multiple sources of real-time data	IDPS SIEM
Detection and Reporting	Detect potentially malicious network activity, notify partner organizations, and share incident information with other EC3s	Sensors monitoring ESInet traffic Analytics and detection tools processing multiple sources of real-time data Shared situational awareness and information sharing environment with other EC3 partners Formal incident response and recovery procedures involving other EC3s, FSLTT partners, and private-sector providers	Partner Outreach Incident Information Sharing IDPS SIEM

Step	EC3 Role	Capabilities Required	Solutions
Response and Recovery	Support ECC/PSAP response and recovery operations, including mitigating threats, restoring service, and conducting after-action analysis	Sensors monitoring ESInet traffic Analytics and detection tools processing multiple sources of real-time data Formal incident response and recovery procedures involving other EC3s, FSLTT partners, and private-sector providers Event analysis escalation to cybersecurity subject matter experts Malware remediation measures (e.g., firewalls, data backups, software patch distribution, managing user-access permissions) Network vulnerability assessment and reporting	Partner Outreach Incident Information Sharing IDPS SIEM

195
196