September 16, 2020

COMMUNICATIONS SECURITY, RELIABILITY, AND INTEROPERABILITY COUNCIL VII

REPORT ON SECURITY RISKS AND BEST PRACTICES FOR MITIGATION IN 9-1-1 IN LEGACY, TRANSITIONAL, AND NG 9-1-1 IMPLEMENTATIONS

Working Group 4: 911 Security Vulnerabilities during the IP Transition

Table of Contents

1 Results in Brief

1.1 Executive Summary

The Commission specifically directed the CSRIC VII to publish a *Report on Security Risks and Best Practices for Mitigation in 9-1-1 in Legacy, Transitional, and NG9-1-1 Implementations,* measuring the risk magnitude and remediation costs within those networks. This report represents the second of three reports on 911 Security Vulnerabilities during the IP Transition and is focused on measuring the security risk within 9-1-1 networks.

Next Generation 9-1-1 has greater scalability and flexibility than the current 9-1-1 environment. The advanced NG9-1-1technology 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. Advanced IP networks supporting NG9-1-1's interconnections enable new response capabilities, but also introduce new opportunities for cyber-attacks that can disrupt PSAP operations. Further, the transition from legacy 9-1-1 networks to NG9-1-1 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 911 systems operate at higher risk."

This report focuses on the cybersecurity risk inherent in any IP-based network or system, with particular focus on the threat surface and potential attack vectors related to Emergency Communications Centers (ECCs). Prior reports published by the FCC educated readers on the various transitional phases involved in migrating from the current legacy 9-1-1 networks to fully operational IP-based next generation networks for 9-1-1. CSRIC VII determined that several of the transitional phases did not materially impact the nature of cybersecurity during the transition, so CSRIC VII consolidated some of the stages and focused on the following phases for cyber education as part of the report and its recommendations:

> **Legacy State**
> *As defined by TFOPA, a Legacy State is characterized as the point in time where 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 State**
> *The Transitional State, as defined for this report, includes the basic groundwork and planning, essential data preparation and foundational IP infrastructure necessary for NG9-1-1. The Transitional State recognizes that the major components of an NG9-1-1 service architecture, i.e., the originating network, the Emergency Services Network, and the PSAP, will evolve at different rates. During the Transitional State, services have begun the migration from the legacy environment to an IP-enabled infrastructure. The Transitional State, as described in this report, assumes that the Emergency Services IP Network (ESInet) is in place supported by the associated*

Next Generation 9-1-1 Core Services that are within the control of the cognizant 9-1-1 authority. PSAPs may have evolved to support multimedia call handling and other NG9-1-1 functionality characteristic of an ECC, or they may retain legacy functionality and interfaces. Likewise, originating networks may or may not have evolved to support NG9-1-1 functionality and interfaces. Infrastructure and applications continue to be refined to incorporate advanced call- and data-delivery interfaces. Business and performance elements are maturing and are reviewed in regular intervals to optimize operations.

End State
The End State is the state in which PSAPs have evolved to become Emergency Communications *Centers and are served by i3 standards-based systems and / or elements, from ingress through multimedia "call" handling. Originating Service Providers are providing SIP interfaces and location information during call set-up time. Nationally, ESInets are interconnected providing interoperability which is supported by established agreements, policies and procedures. All systems in the End State are NG9-1-1 Compliant.*

This report is designed to address security considerations for each phase, but it is also intended to address the larger threat landscape and how industry and public safety can work together to implement appropriate measures based on a combined threat analysis and approach. It should be noted that the actual transition from legacy networks through to an NG9-1-1 End State will introduce opportunities for hackers to compromise our 9-1-1 Centers. During transitions involving computer upgrades, especially those requiring significant upgrades of network infrastructure as will be the case for NG9-1-1, modifications to common cybersecurity protections, such as firewalls and end point security systems, create the opportunity for human error. Hackers are constantly watching for openings – vulnerabilities being exposed by inappropriate or incorrect changes to network systems. It is appropriate that the Commission should provide caution and guidance for public safety agencies that go through these transitions so that they can better prepare for change through planning and adoption of recommended best practices.

To ensure that the transition from legacy 9-1-1 to NG9-1-1 is secure, Section 5 of the report provides an analysis of the importance of cybersecurity during the transition to NG9-1-1, and Section 6 identifies specific attack surfaces and describes cybersecurity models that can be used by public safety to improve their security posture. Section 7 provides Use Cases for various types of security threats and includes recommendations for mitigation strategies for each Use Case. Timely and thorough action to manage the impact of cyber incidents is a critical component of the response process and it takes everyone being involved for a response plan to work. This is accomplished through the development of cyber incident response goals; and Section 7 of the report also provides the reader with guidance on Protection, Detection, Response, and Recovery Functions.

In addition to focusing on security vulnerabilities, CSRIC VII also reviewed the existing FCC Best Practices related to cybersecurity and public safety. The review provided an opportunity to recommend enhancements to specific FCC Best Practices, and the report also includes references to Best Practices that exist in other industry forums specific to cyber issues.

Everything in 9-1-1 should be absolutely secure and 100% available because 9-1-1 is a critical public safety service. This report provides excellent guidance to ensuring 9-1-1 systems are secure. However, it is not reasonable to expect that every entity in the 9-1-1 community will achieve a high level of security overnight or over the same timescale; much like various jurisdictions move forward in the NG9-1-1 transition at different times and at different rates.

Section 0 of the report includes the following CSRIC recommendations are targeted to the Public Safety community:

- Implementing the appropriate industry-recognized cybersecurity controls in their entirety where possible, and in phases if necessary, during the transition.
- Organizations implement basic security controls, regardless of size, in a legacy environment.
- NG9-1-1 networks implement foundational security controls and some of the organizational security controls.
- Implement Best Practices as indicated in Report 2 and Report 3.

Section 0 of the report also provides recommendations to the Commission for future initiatives:

- Review and revise this report to accommodate changes in cybersecurity advancements, improving on the security recommendations for 9-1-1 systems.
- Review cybersecurity aspects of future technologies impacting Public Safety:
    - 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,
    - 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 serves as the foundation for educating the Public Safety community on cybersecurity risks and should assist the Commission with future initiatives related to cybersecurity and 9-1-1.

2 Introduction

The FCC directed CSRIC VII 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 Next Generation 9-1-1 (NG9-1-1). The FCC further directed CSRIC VII to identify security risks in legacy

9-1-1 networks, transitional 9-1-1 networks, and NG9-1-1 networks and to recommend best practices to mitigate risks in these three areas. Finally, the Commission asked CSRIC VII to place the vulnerabilities on a scale that accounts for both risk level and remediation expense, and assigned the following milestones for the reports involved:

***Milestones**:*

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

The US Department of Homeland Security (DHS) acknowledges that "[t]he advent of Next Generation 911 (NG911) systems, which operate on an Internet Protocol (IP) platform, enables interconnection on with a wide range of public and private networks, such as wireless networks, the Internet, and regular phone networks. NG911 systems will enhance the current capabilities of today's 911 networks, allowing compatibility with more types of communication, providing greater situational awareness to dispatchers and emergency responders, and establishing a level of resilience not previously possible."[1] Nevertheless, they also observe that, ". . . 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. Past events have proven 911 systems are attractive targets for cyber-attacks."[2]

The transition from legacy 9-1-1 networks to the NG9-1-1 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 911 systems operate at higher risk."

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. Thus, understanding the extent and nature of interoperability between 9-1-1 systems plays an important role in cyber-protecting our public safety infrastructure.

The existence of diverse systems will put the nation's 9-1-1 system at risk until the transition can be completed. In the world of technology, system transition phases are notoriously rife with risks that do not exist in either the beginning state or in the end state. Therefore, having in place security mechanisms to secure full system functionality during the transition phase will be essential to the well-ordered functioning of the system.

[1] US Department of Homeland Security, Office of Emergency Communications, "Cyber Risks to Next Generation 911, see: https://www.911.gov/pdf/OEC_NG911_Cybersecurity_Primer_041216_508_compliant.pdf
[2] Ibid.

2.1 CSRIC VII Structure

CSRIC VII was established at the direction of the Chairman of the Federal Communications Commission (FCC) 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 ensure the 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	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, America's Public Television Stations	Chair: Lee Thibaudeau, Nsight	Chair: Farrokh Khatibi, Qualcomm	Chair: Mary Boyd, West Safety Services	Chair: Pat Roberts, Florida Association of Broadcasters	Chair: Danny McPherson, Verisign
FCC Liaison: James Wiley	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	CenturyLink
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)[3]	SecuLore Solutions
Krisztina Pusok	American Consumer Institute
Theresa Reese	Ericsson
Rasoul Safavian	Federal Communications Commission (FCC)
Charlie Sasser	National Association of State Technology Directors (NASTD)
Andre Savage	Cox Communications
Dorothy Spears-Dean	National Association of State 911 Administrators
Leslie Sticht	State of Minnesota
Mark Titus	AT&T
Brian Trosper (Alternate: Bill Mertka)	Verizon
Jeff Wittek	Motorola Solutions
Jackie Wohlgemuth	ATIS

Table 2 - List of Working Group Members

3 Objective, Scope, and Methodology

3.1 Objectives

Report on the Security Risks and Best Practices for Mitigation in 911 in Legacy, Transitional, and NG911 Implementations

In 2009, the National E9-1-1 Implementation Coordination Office (now known as the National 911 Program) published *A National Plan for Migrating to IP-Enabled 9-1-1 Systems*[4]. In that Plan, the Office outlined potential benefits of such a migration. "PSAP Connectivity and Interoperability" was identified as a specific benefit.

Today, cybersecurity[5] is a function of not only the nature of the technology involved, but also of its function. NG9-1-1 is a good example of that. NG9-1-1 has greater scalability and flexibility than the current 9-1-1 environment. NG9-1-1 also has a greater potential to increase public and first responder safety through interconnectivity and interoperability than the current 9-1-1 environment. With IP-enabled 9-1-1, the physical location of an Emergency Communications Center (ECC)[6] becomes immaterial. IP-enabled technology will allow callers to reach 9-1-1 call takers regardless of the ECC location. NG9-1-1 will allow ECCs to transfer and share information with other call centers or response agencies more quickly and with greater accuracy by way of shared and accurate Geographic Information System (GIS) based routing, regardless of location, and to deliver access to crucial data at a level rarely available today. The ability to

[3] Tom Breen represented Comtech on Working Group 4 from 7/2019 through 7/2020.

[4] https://www.911.gov/pdf/ICO_National_Plan_Migrating_IP_911_Systems_2009.pdf

[5] 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

[6] An ECC is a more comprehensive and contemporary term for the classic PSAP, or public safety answering point. An ECC performs the functions of a PSAP but includes additional functionality associated with NG9-1-1 and NG public safety that was not, by and large, deployed in classical PSAPs.

transfer 9-1-1 calls within and among jurisdictions along with all collected data provides resilience that currently does not exist, but that may be essential in the event of call overload or ECC damage.

DHS notes that "[t]raditional 911 services typically operate over standard voice-based telephone networks and use software, such as computer-aided dispatch systems, that operate on closed, internal networks with little to no interconnections with other systems. NG911's interconnections enable new response capabilities . . . However, they also represent new vectors for attack that can disrupt or disable PSAP operations, broadening the concerns of—and complicating the mitigation and management of—cyber risks across all levels of government."[7]

Interoperability continues to be at the heart of the migration to NG9-1-1. As noted above, the Commission specifically directed CSRIC VII to report on the "Security Risks and Best Practices for Mitigation in 911 in Legacy, Transitional, and NG911 Implementations".

3.2 Scope

The transition from legacy 9-1-1 circuit switched systems to IP-based NG9-1-1 systems provides an opportunity to assess the security vulnerabilities of these systems during that transition. That migration is not a simple process. While today's environment is what we have, and tomorrow's end-state NG9-1-1 will be standards based, "transition" will involve a variety of different deployment scenarios based upon local conditions, resources, and needs. That potentially sets-up a complex array of security threats when different systems at different states of transition interoperate with each other.

This report focuses on the cybersecurity risk inherent in any IP-based network or system, with particular focus on the threat surface and potential attack vectors as they relate to ECCs. As noted above, NG9-1-1 will involve a phased transition, with multiple levels, and types, of ECCs co-existing for some time to come. The integration of a singular cyber defense program into the complex fabric of multi-faceted NG9-1-1 systems, from legacy to transitional and into a true end-state, is not possible. What is possible is the implementation of multiple recommendations, creation and integration of cooperative defensive systems, and a focus on prevention rather than just response. This report will provide input on each of these areas, as well as recommendations, best practices, and options for the 9-1-1 community.

3.3 Methodology

The Commission directed CSRIC VII to draft a Report on Security Risks and Best Practices for Mitigation in 9-1-1 in Legacy, Transitional, and NG9-1-1 Implementations. This report represents the cumulation of research into potential current, and future security risks. Mitigation is discussed in-line with identified risks.

3.3.1 Transition Paradigm

In its "Report on the Current State of Interoperability in the Nation's 911 Systems," CSRIC VII

[7] US Department of Homeland Security, Office of Emergency Communications, "Cyber Risks to Next Generation 911, see: https://www.911.gov/pdf/OEC_NG911_Cybersecurity_Primer_041216_508_compliant.pdf

looked to the "maturity states" adopted by the FCC's Task Force on Optimal Public Safety Answering Point Architecture:[8] The TFOPA activity defined states ranging from today's legacy state, through foundational, transitional, and intermediate states, culminating in jurisdictional and nation-wide "end states." The previous CSRIC VII report assumed that the interoperability envisioned by fully deployed NG9-1-1 (i.e., "end state") would vary depending upon legacy transition progress to NG9-1-1 (i.e., "maturity level"). For this report, however, 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," resulting in the three main states described below. CSRIC VII assumed that cybersecurity requirements for each state would vary to some degree. The report is designed to address security considerations in that fashion but is also intended to address the larger threat landscape and how industry and public safety can work together to implement appropriate measures based on a combined threat analysis and approach.

3.3.2 Legacy State

As defined by TFOPA, a Legacy State is characterized as the point in time where 9-1-1 services are provided by the traditional incumbent local exchange carrier (ILEC) with circuit-switched infrastructure and Automatic Location Identification (ALI) database and circuits.

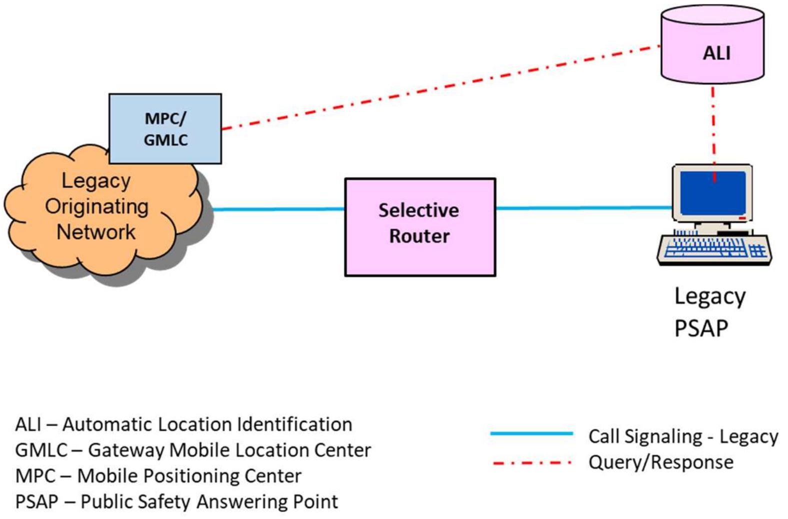

ALI
MPC/ GMLC
Legacy Originating Network
Selective Router
Legacy PSAP
ALI – Automatic Location Identification
GMLC – Gateway Mobile Location Center
MPC – Mobile Positioning Center
PSAP – Public Safety Answering Point
Call Signaling - Legacy
Query/Response

Figure 3-1 Legacy State

[8] 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, https://transition.fcc.gov/pshs/911/TFOPA/TFOPA_WG2_Supplemental_Report-120216.pdf. This report in turn based their NG9-1-1 maturity states descriptions on the National 911 Program's report on a national NG9-1-1 cost study underway at that time. See: National 911 Program, https://www.911.gov/project_nextgeneration911coststudy.html
The URL for the actual PDF is:
https://www.911.gov/pdf/Next_Generation_911_Cost_Estimate_Report_to_Congress_2018.pdf

As depicted in Figure 3-1, Selective Routers (SRs) (also known as E9-1-1 Tandems) are a critical element of legacy emergency services networks that support Enhanced 9-1-1 (E9-1-1) Service. SRs are specially-equipped central offices that provide the switching of 9-1-1 calls. Selective routing is the process by which 9-1-1 calls are routed to the appropriate PSAP (or other designated destination) based on the caller's location. For emergency calls that originate in legacy wireline networks, the caller's location is determined by their 10-digit telephone number or Automatic Number Identification (ANI). For emergency calls that originate in legacy wireless networks, selective routing is done based on a 10-digit location key that represents the cell site and sector that the caller is calling from. In addition to providing selective routing functionality, SRs control the delivery of voice calls to the PSAP, as well as emergency call transfer and certain maintenance functions for each PSAP.

In the Legacy State, SRs typically receive emergency calls over dedicated Multi-Frequency (MF) (Centralized Automatic Message Accounting [CAMA] or Feature Group-D) or Signaling System No. 7 (SS7) trunk groups from wireline end offices and Mobile Switching Centers (MSCs) in legacy originating networks. They use information received in incoming signaling to interact with a Selective Routing Database (SRDB) that identifies the PSAP that serves the area in which the call originated. SRs deliver the emergency call to the PSAP, typically over traditional CAMA-like or Enhanced MF interfaces, with a location key that allows the PSAP to query an Automatic Location Identification (ALI) database for the caller's location information via a separate data interface. In the case of wireline emergency callers, the ALI database contains static telephone number-to-street address mappings. In support of emergency calls from wireless callers, the ALI system contains mappings from a location key to steering data that triggers the ALI system to query a Mobile Positioning Center (MPC)/Gateway Mobile Location Center (GMLC) in the legacy wireless originating network to obtain location associated with the emergency caller. The PSAP uses location information returned to it by the ALI system to support the dispatch of emergency personnel.

3.3.3 Transitional State

The Transitional State, as defined for this report, includes the basic groundwork and planning, essential data preparation and foundational IP infrastructure necessary for NG9-1-1. The Transitional State recognizes that the major components of an NG9-1-1 service architecture, i.e., the originating network, the emergency services network, and the PSAP, will evolve at different rates. During the Transitional State, services have begun the migration from the legacy environment to an IP-enabled infrastructure. The Transitional State, as described in this report, assumes that the Emergency Services IP Network (ESInet) is in place supported by the associated Next Generation Core Services that are within the control of the cognizant 9-1-1 authority. PSAPs may have evolved to support multimedia call handling and other NG9-1-1 functionality characteristic of an ECC, or they may retain legacy functionality and interfaces. Likewise, originating networks may or may not have evolved to support NG9-1-1 functionality and interfaces. Infrastructure and applications continue to be refined to incorporate advanced call- and data-delivery interfaces. Business and performance elements are maturing and are reviewed in regular intervals to optimize operations.

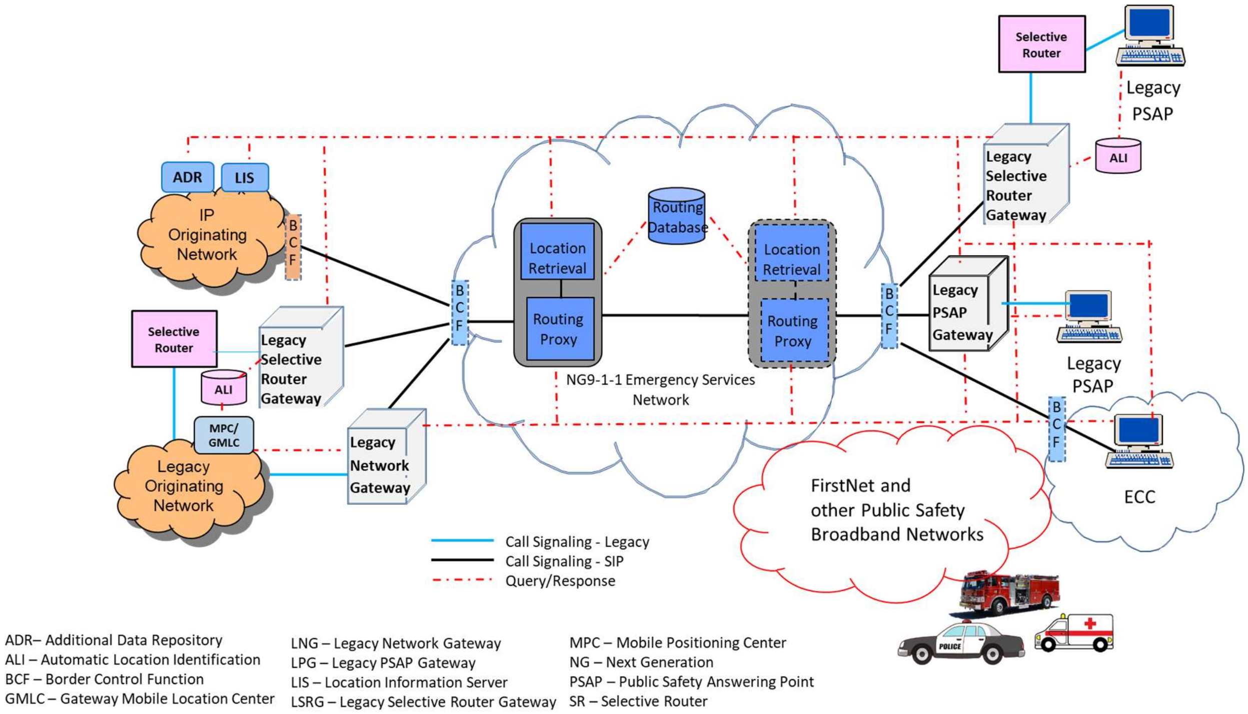

Selective Router
Legacy PSAP
ALI
Legacy Selective Router Gateway
ADR
LIS
IP Originating Network
BCF
Location Retrieval
Routing Proxy
Routing Database
Location Retrieval
Routing Proxy
BCF
Legacy PSAP Gateway
Legacy PSAP
Selective Router
Legacy Selective Router Gateway
ALI
MPC/ GMLC
Legacy Originating Network
Legacy Network Gateway
NG9-1-1 Emergency Services Network
BCF
FirstNet and other Public Safety Broadband Networks
BCF
ECC
POLICE
Call Signaling - Legacy
Call Signaling - SIP
Query/Response
ADR– Additional Data Repository
ALI – Automatic Location Identification
BCF – Border Control Function
GMLC – Gateway Mobile Location Center
LNG – Legacy Network Gateway
LPG – Legacy PSAP Gateway
LIS – Location Information Server
LSRG – Legacy Selective Router Gateway
MPC – Mobile Positioning Center
NG – Next Generation
PSAP – Public Safety Answering Point
SR – Selective Router

Figure 3-2 Transition to NG9-1-1

During the Transitional State, as illustrated in Figure 3-2, there will continue to be legacy wireline and wireless originating networks deployed after emergency service networks and a significant number of PSAPs have evolved to support NG9-1-1 architectures. Since ECCs served by NG9-1-1 emergency services networks will need to be able to receive emergency calls that originate on these legacy networks, gateway functionality will be a required part of a transitional NG9-1-1 Service Architecture. This gateway functionality must include signaling interworking to convert the incoming MF or SS7 signaling generated by a legacy originating network to the IP-based (i.e., Session Initiation Protocol [SIP]) signaling supported by an NG9-1-1 emergency services network. In addition, since routing within the NG9-1-1 emergency services network will be based on location (in the form of a street address or geo-coordinates), a gateway element on the ingress side of an NG9-1-1 emergency services network must support the ability to use the information provided by a wireline switch or MSC in call setup signaling (e.g., calling number/ANI, pseudo ANI/location key) to retrieve location information that can be used as input to routing determination. Based on the routing location provided, the routing determination function will identify which emergency services network should handle the call. The same routing location will also be used to support routing within the NG9-1-1 emergency services network.

Gateway functionality will also be needed to enable interactions between NG9-1-1 emergency services network elements (and the PSAPs they serve) and legacy systems, such as MPCs/GMLCs, to support the retrieval of location to support the dispatch of emergency personnel. The type of gateway that the legacy originating network interconnects with will depend on where the legacy originating network is in its evolution. Legacy originating networks that are still connected to SRs will utilize a Legacy Selective Router Gateway between the SR and the NG9-1-1 emergency services network to support the necessary interworking functionality. Alternatively, legacy originating networks at a different phase of evolution may no longer interconnect with SRs and may instead interconnect directly with a Legacy Network Gateway to gain access to the NG9-1-1 emergency services network.

In addition to gateway functionality on the ingress side of an NG9-1-1 emergency services network, during transition there will be a need to support gateway functionality on the egress side of the NG9-1-1 emergency services network. While an increasing number of PSAPs will evolve to become ECCs over time, NG9-1-1 emergency services networks must be able to deliver emergency calls to interconnected legacy PSAPs. The NG9-1-1 Service Architecture must therefore include a functional element that will provide signaling interworking and other 9-1-1-specific functionality necessary for emergency calls routed via the NG9-1-1 emergency services network to be delivered to and handled by legacy PSAPs without requiring changes to legacy PSAP equipment. Calls routed via an NG9-1-1 emergency services network and delivered to a legacy PSAP must undergo signaling interworking to convert the incoming IP-based (i.e., SIP) signaling supported by the NG9-1-1 emergency services network to the MF signaling supported by the legacy PSAP. Functionality must also be applied by the NG9-1-1 emergency services network to 9-1-1 calls to allow the legacy PSAP to experience call delivery, ALI data retrieval, and feature activation the same way as they do in an E9-1-1 environment. The type of gateway system used to support the delivery of 9-1-1 calls routed via an NG9-1-1 emergency services network to a legacy PSAP will depend on what stage of evolution to an ECC the PSAP is in. If the PSAP is still served by an SR, 9-1-1 calls will need to be routed by the NG9-1-1 emergency services network via a Legacy Selective Router Gateway to the SR that serves the legacy PSAP. If the legacy PSAP is no longer served by an SR, a Legacy PSAP Gateway will support call delivery using MF signaling to the legacy PSAP as if it were an SR, and location/data delivery to the legacy PSAP via legacy ALI interfaces, as if it were an ALI system. Legacy PSAP Gateways or Legacy Selective Router Gateways operating on the egress side of the NG9-1-1 emergency services network will also need to support interfaces to elements in an IP originating network or to Legacy Network Gateways or Legacy Selective Router Gateways operating on the ingress side of the NG9-1-1 emergency services network to support the retrieval of location or other data.

3.3.4 End State

The End State is the state in which PSAPs have evolved to become ECCs and are served by i3 standards-based systems and / or elements, from ingress through multimedia "call" handling. Originating Service Providers are providing SIP interfaces and location information during call set-up time. Nationally, ESInets are interconnected providing interoperability which is supported by established agreements, policies, and procedures. All systems in the End State are NG9-1-1 Compliant.

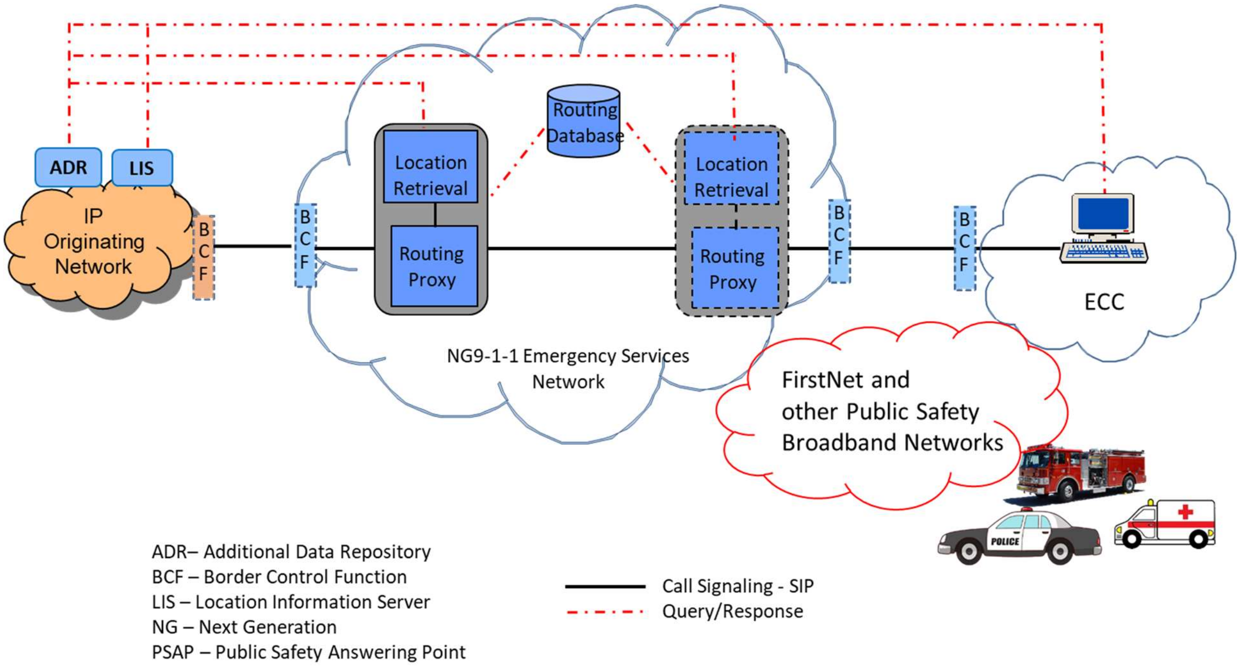

ADR
LIS
IP Originating Network
BCF
BCF
Location Retrieval
Routing Proxy
Routing Database
Location Retrieval
Routing Proxy
BCF
BCF
ECC
NG9-1-1 Emergency Services Network
FirstNet and other Public Safety Broadband Networks
POLICE
ADR– Additional Data Repository
BCF – Border Control Function
LIS – Location Information Server
NG – Next Generation
PSAP – Public Safety Answering Point
Call Signaling - SIP
Query/Response

Figure 3-3 End-State NG9-1-1

The end-state NG9-1-1 architecture depicted in Figure 3-3 assumes that the originating network supports IP connectivity and NG9-1-1 “call” and data processing functionality, an NG9-1-1 emergency services network is in place, and legacy PSAPs have evolved to become ECCs capable of processing multimedia communications from emergency callers, as well as location and other data associated with 9-1-1 originations. The ECCs will use all of this information to support the dispatch of emergency personnel and the conveyance of critical incident data to first responders.

In an end-state NG9-1-1 environment, an emergency request will be forwarded by an IP originating network (via a Border Control Function) to a routing proxy in an NG9-1-1 emergency services network with callback information and location information. The location may be delivered “by-value” (i.e., where the civic location/street address or geo-coordinate location is contained within the SIP signaling message) or “by-reference” (i.e., the SIP signaling message contains a “pointer” or “reference” to the location information that includes the address of the element from which the location information can be obtained and a “key” to the data). The routing proxy uses the location information received in incoming SIP signaling (location-by-value) or obtained by dereferencing a location-by-reference to query a GIS-based routing database. The routing response contains the address of the “next hop” in the call path. Call routing may also be influenced by policy routing rules accessed by the routing proxy. The routing proxy forwards the emergency call/session request (with the same callback and location information as it received in incoming SIP signaling) to the “next hop” element based on the address received in the response from the routing database and any applicable routing policy. The “next hop” element may be the ECC or it may be another routing proxy in the call path, depending on the way the NG9-1-1 Service Architecture is implemented. Ultimately, the emergency request is delivered to the ECC with the same callback and location information that was initially delivered to the routing proxy.

The ECC will use the information received via signaling, as well as information received via other media and through interactions with the emergency caller to determine the type of emergency response required and the location to which the response should be directed. The ECC will assess the availability of emergency response resources required and dispatch the appropriate emergency response providers. In an end-state NG9-1-1 environment, critical incident data will be shared between affected agencies and with first responders using standard data formats and conveyance mechanisms.

4 Background

9-1-1 and public safety have been a very high priority for the FCC since the early 1990's. CSRIC VI addressed 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." Specifically, CSRIC VI was asked to:

- Review existing Best Practices regarding overall monitoring, reliability, notifications, and accountability in preventing 9-1-1 outages in transitional NG9-1-1 environments.
- Develop additional guidance on Best Practices regarding overall monitoring, reliability, notifications, and accountability in preventing 9-1-1 outages in transitional NG9-1-1 environments.
- Identify risks associated with transitional 9-1-1 systems that could result in disruptions to 9-1-1 service.
- Make recommendations to protect the NG9-1-1 network, including recommendations for Best Practices and standards development.
- Study specific actions that originating Service Providers, 9-1-1 System Service Providers and other entities in the 9-1-1 call chain should take to detect and deter outage precursors before 9-1-1 calls are delivered to the ESInet gateway.
- Recommend actions the FCC could take to encourage the private sector to detect or deter threats to 9-1-1 before they reach the ESInet perimeter. The focus would be on Identifying tools that are already available or not burdensome to implement.
- Recommend a "NG9-1-1 readiness checklist" for small carriers analogous to the one the TFOPA developed for PSAPs

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." 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.

CSRIC VI also recognized that while cybersecurity considerations are an important part of the transition to NG9-1-1, neither the charter, nor the report, had focused on cybersecurity. In reality, the topic required very specialized expertise. In the report, CSRIC VI recommended that stakeholders take deliberate steps to consider the cybersecurity implications introduced by the transition to NG9-1-1. CSRIC VI also recommended that a future CSRICs focus on NG9-1-1 related cybersecurity challenges and develop Best Practices as appropriate.

Following the CSRIC VI recommendations, the Commission structured the CSRIC VII initiative to follow the recommendations of the prior CSRIC VI Report resulting in the action items identified in Section 3.1 above. The FCC directive to CSRIC VII as the result of the work accomplished in CSRIC VI was as follows:

The FCC directs 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 (NG911). (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)*
- *In addition, CSRIC VII will place the vulnerabilities on a scale that accounts for both risk level and remediation expense. (March 2021)*

These action items will be delivered to CSRIC VII starting in March 2020, with a final completion date of March 2021. The March 2020 report focused on the findings resulting from an assessment of the current state of 9-1-1 systems interoperability, including for legacy 9-1-1 networks, transitional 9-1-1 networks, and NG9-1-1. The status of interoperability provides a foundation for identifying security risks within the transitional 9-1-1 networks and making best practice recommendations to mitigate these risks.

5 Analysis of the Importance of Cybersecurity to the NG9-1-1 Transition

- Transition of emergency networks and citizen-to-authority communications from traditional telephony technology to IP-based infrastructures brings many benefits, but also challenges, and high on the list of those challenges is openness to cybersecurity breaches and attacks on information security (InfoSec) that did not exist in the legacy 9-1-1 system
- Providing adequate cybersecurity and privacy mechanisms to protect the new infrastructure and the data traversing it will be a huge challenge that must be faced and surmounted for the NG9-1-1 rollout to ultimately be successful
- While overall NG9-1-1 security has many aspects, including physical, operational, and cyber, the new challenges for public safety will largely lie in the cyber domain
- In the new era, public safety agencies will have to be “cybersecurity savvy” and able to research, develop, and maintain adequate cybersecurity and privacy protection, or know enough to select the proper vendors to provide these services. Failure to do so will vitiate the hoped-for benefits from the transition, and would very likely lead to a system with degraded functionality
- Adequate cybersecurity and privacy protection in the era of IP-based systems involves more than deploying security systems technology like firewalls and intrusion detection systems; the state of the art of cybersecurity protection is more challenging and complicated than was envisioned when NG9-1-1 standards development was first undertaken and protecting today’s systems in the current threat environment will require ECCs to go beyond mere standards compliance and will require implementing and staying current with industry best practice
- Policy, operational procedures, threat intelligence and assessment and information sharing mechanisms with friendly stakeholders must all be put in place in order to achieve a security posture at each ECC adequate to protect NG9-1-1 systems from the threat rich environments they will be operating in
- ***EVERY*** entity in the public safety services ecosystem will have to develop and maintain its own security and privacy controls, based on standards and best practices to the extent possible and developed in coordination with other stakeholders in order to ensure the success of the transition.

6 Introduction to NG9-1-1 Cybersecurity Considerations

As noted in previous work by other FCC Advisory Committees, specifically the Task Force on Optimal PSAP Architecture (TFOPA), “Cyber risk management strategies are being developed for the communications sector that will benefit the NG9-1-1 ecosystem as a whole."[9] As a result, the intent of CSRIC VII is not to "reinvent the wheel;" rather it is to reinforce existing valid recommendations, further define the threat landscape specific to emergency communications, and provide updated recommendations for mitigating the threat, including updates to recommendations from previous work. A recognized and widely adopted approach to cyber defense is detailed in the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and that work will be referenced here. In addition, there is ongoing work from other organizations including the U.S. Department of Homeland Security (DHS), the Association of Public Safety Communications Officials (APCO), and the National Emergency Number Association (NENA) that will be referenced in this report.

As also noted in the first TFOPA report, "Cyber risk management strategies must be implemented in support of PSAP operations, while still taking into consideration available PSAP resources and levels of expertise. Accordingly, it is necessary to think 'outside the box' when considering cybersecurity architectures and developing solutions." [10]

We have decided to take a slightly different approach to identifying threats, and mitigation, from previous reports. In our work we have chosen to first identify the attack surface(s), then specify how each might relate to Emergency Communications in legacy, transitional, and end-state stages. In our research, an excellent summary of why we chose this approach is found in the following statement:

> ***How would your security program run differently if your perspective was shaped around attack-surface reduction?***

6.1 9-1-1 Attack Surfaces

First off, what does "attack surface" mean? This term gets thrown around plenty within the InfoSec community, but are all commentators talking about the same thing? Often, the first term mentioned in a discussion like this is that of attack vectors. To simply define it, an attack vector really isn't much more than some avenue that a bad actor can use to exploit systems, networks, and information.

The attack surface, then, is just the sum of all the attack vectors that exist for an organization — the total surface area of potential system exposure, be it systems in the data center, laptops in the field, cloud applications, connected industrial systems, or any combination of these hybrid environments that organizations may have.

[9] TFOPA WG1: Optimal Cybersecurity Approach for PSAPs, Final Report, dated December 10, 2015, p. 4.

[10] TFOPA WG1: Optimal Cybersecurity Approach for PSAPs, Final Report, dated December 10, 2015 , p. 4.

6.1.1 Attack Surface Descriptions

A good way to look at “attack surfaces” within a NG9-1-1 context is to consider the seven (7) facets of “attack surface” in the emerging NG9-1-1 system. Figure 6-1 sums these up:

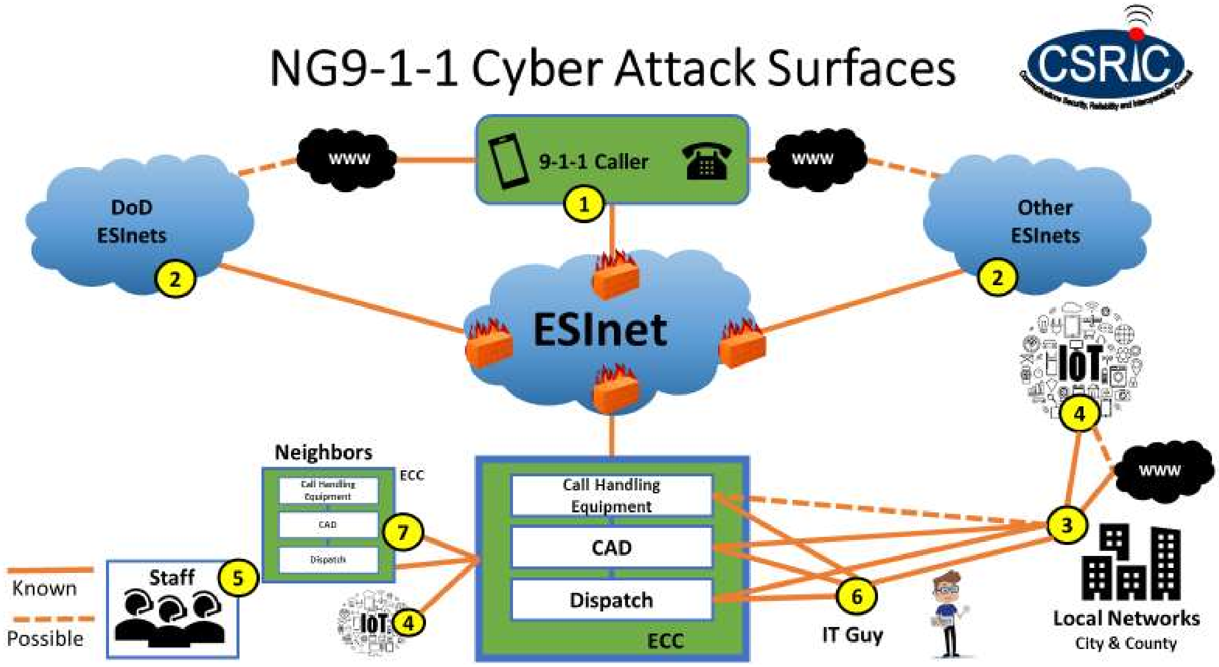
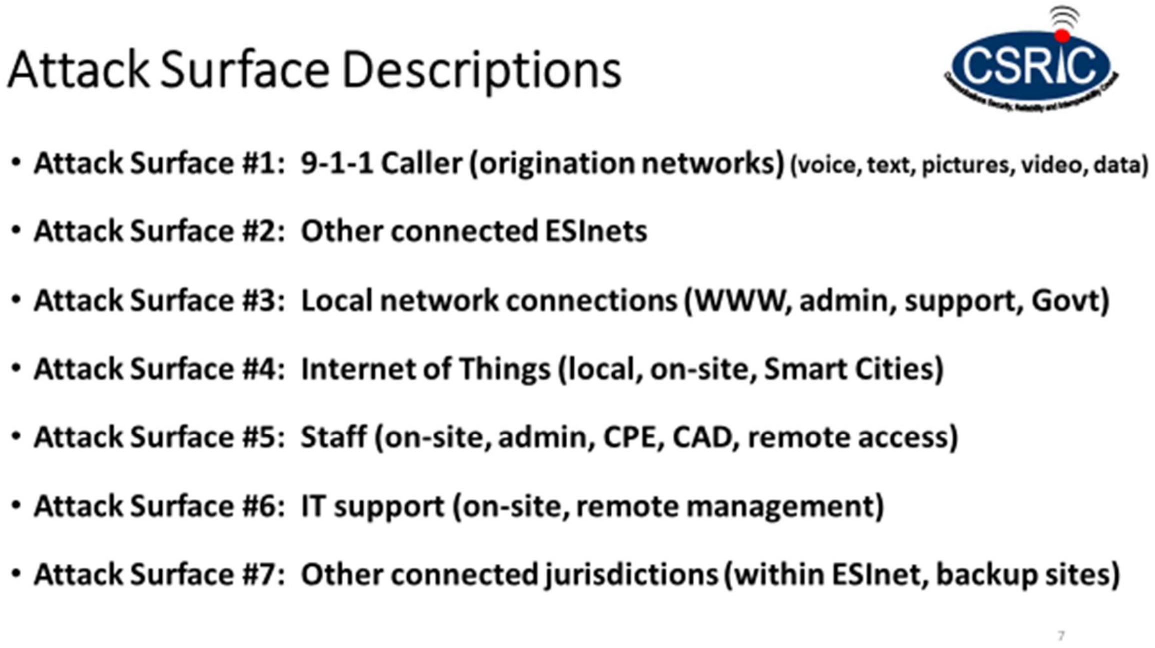


Figure 6-1 The Seven NG9-1-1 Cyber Attack Surfaces



Attack Surface Descriptions

- **Attack Surface #1: 9-1-1 Caller (origination networks)** (voice, text, pictures, video, data)
- **Attack Surface #2: Other connected ESInets**
- **Attack Surface #3: Local network connections (WWW, admin, support, Govt)**
- **Attack Surface #4: Internet of Things (local, on-site, Smart Cities)**
- **Attack Surface #5: Staff (on-site, admin, CPE, CAD, remote access)**
- **Attack Surface #6: IT support (on-site, remote management)**
- **Attack Surface #7: Other connected jurisdictions (within ESInet, backup sites)**

7

6.1.1.1 Attack Surface #1 – The 9-1-1 "Caller"

The 9-1-1 "Caller" represents three distinct types of threats to an ECC. Content, interconnection method, and frequency of 9-1-1 "calls" each provide unique opportunities for a Threat Actor to impair the performance of an ECC.

In a Legacy 9-1-1 environment, a 9-1-1 interaction can only be initiated via a voice call – even TTY text-based communications are conducted using BAUDOT tone exchanges over a connected voice path. Thus, Legacy PSAPs only accept voice-based content; as such, the content poses minor or non-existent cyber threats to a PSAP. As we transition to NG9-1-1, a caller in a local jurisdiction will be able to initiate a 9-1-1 interaction using various forms of multimedia; and the transition to NG9-1-1 may start to introduce some of these multimedia methods. For example, many 9-1-1 Emergency Communication Centers have already implemented Text-to-911 capabilities, allowing a caller to initiate a call for help using a text message directed to the number "9-1-1" and the underlying wireless communication systems use wireless location and routing techniques to deliver the 9-1-1 text message to the responding 9-1-1 ECC. This is an example of transition to NG9-1-1 and represents an example of the 9-1-1 "Caller" attack surface. It is possible to embed malicious links in a 9-1-1 text message, and thus Text Messages become a cyber-attack source for a 9-1-1 ECC that accepts text messages. As we continue to transition to full NG9-1-1 capabilities, an ECC will be able to receive an increasing number of media types such as pictures, video, and even data from sources such as automobiles or homes that will serve as proxies for the caller trying to reach the ECC in an emergency context. From a cybersecurity perspective, the "9-1-1 Caller" is an unknown. Technology being used to initiate a 9-1-1 call using any of the aforementioned forms of multimedia could be malicious in nature either by direct intent of the caller or because of some interim interaction with a malicious actor that transforms the media with the intent of causing harm to the ECC. As such, the multimedia content being used to initiate the 9-1-1 interaction becomes a content-based Attack Surface of the ECC.

Communications from a 9-1-1 caller start from an Originating Service Provider (OSP). The interconnections along the path between the OSP and the 9-1-1 ECC are touch-points and thus should be treated as Attack Surfaces of the ECC. These interconnection methods are heavily dependent upon the type of media being exchanged with an ECC. Most OSPs today will interconnect with ECCs using Time-Division Multiplexing (TDM) techniques. Such interfaces pose minor or non-existent cyber threats to an ECC. However, even voice calls can be conducted over IP-based interfaces. With the advent of Voice-over-IP (VoIP) technologies, the interconnection points between OSPs and ECCs can move to IP-based communications, so this transition to VoIP represents an expansion of the Attack Surface. As the NG9-1-1 call content transitions from voice-only to a broad array of multimedia content, the interconnection methods will transition to IP-based communications techniques that will transport this expanded multimedia content. This will effectively expand the ECC Attack Surface even further as various IP-based interconnection points are deployed.

Finally, the frequency of 9-1-1 “calls” will always pose a threat to PSAP/ECC performance because an ECC has a limited number of telecommunicators who can respond to a 9-1-1 call, regardless of content type of interconnection method. If the number of 9-1-1 “calls” exceeds the capacity of the PSAP’s/ECC’s telecommunicators, the PSAP/ECC is virtually unable to respond to additional 9-1-1 requests. This becomes a type of Denial of Service and can happen with Voice, TTY or any form of multimedia exchange. With the introduction of NG9-1-1 technologies, technology may be able to assist with triaging 9-1-1 “calls” and provide other methods of gathering information or managing emergency response that could potentially mitigate such vulnerabilities. Regardless, the frequency of 911 “calls”, regardless of media type, must be considered an Attack Surface of the ECC.

6.1.1.2 Attack Surface #2 – Connected ESInets

The NG9-1-1 network is often described as a “network of networks” and simply indicates that the NG9-1-1 system will consist of interconnected sub-networks, with each sub-network having a specific function related to the transport and handling of a 9-1-1 interaction initiated by the form of multimedia. The Emergency Services IP Network (ESInet) is the network responsible for transporting the multimedia within the ECC and can also deliver the multimedia to neighboring ECCs by interconnecting the ESInets of the ECCs involved. These interconnection points are, by definition, data connection points and therefore become an Attack Surface in a Cybersecurity context. An NG9-1-1 ECC must assume that the interconnected ESInet could be compromised and thus the ECC must adopt cybersecurity protections against possible cyber-attacks that may originate from the neighboring ECCs. In this regard, the ECC is no different than worries we have in today’s internet where a device within a network managed by an Internet Service Provider (ISP) can be infected by a device or server in a neighboring ISP. The network interconnection facilitates the transmission of malware, and every ISP has an obligation to provide protections for the computer systems it hosts. In this regard, an ECC’s ESInet would have the responsibility of protecting the computer systems within the ECC it serves; and neighboring ESInets would be viewed as possible attack surfaces of the ECC.

6.1.1.3 Attack Surface #3 – Local Network Connections

Our legacy PSAPs provide access to local First Responders; as such, almost every legacy PSAP in the nation is embedded within a local city, county or Emergency Communications District that has a broader set of responsibilities beyond just the PSAP's functions. For example, a 9-1-1 call may require access to local resources or the local network connections provided to the legacy PSAP or ECC. These connections may be the way the PSAP/ECC receives access to the World Wide Web, Poison Control Databases, Criminal Justice Information Services (CJIS), social media, vendor support systems and numerous other data and communication systems that could be important to the normal operations of the PSAP/ECC. These Local Network Connections would provide various forms of media to the PSAP/ECC and would be a possible source of a cyber-attack, making these Local Network Connections an Attack Surface for the PSAP/ECC.

6.1.1.4 Attack Surface #4 – Internet of Things (IoT)

Rapid advances in computer technologies has introduced a wide array of devices that are becoming ever more important in providing emergency response services. Camera systems, arrays of detectors, monitoring systems, and even media recording devices are all evolving to provide more functionality, greater convenience and broader use scenarios. Many such systems will continue to be interconnected into our Legacy PSAPs and NG9-1-1 ECCs and the emergence of 5G is rapidly increasing the number and variety of these IoT devices. Over the last decade, we have seen numerous ways in which such systems have been compromised and used as attack vectors in a cyber-connected world. Because these devices are often purchased and deployed as independent projects within or in conjunction with ECCs, it is wise to consider these systems as an independent Attack Surface and to consider them from three perspectives: independent external systems interconnected to the ECC, embedded systems interconnected to the ECC via Smart Cities initiatives, and local devices embedded within the ECC itself to provide specific functions such as local monitoring, maintenance, recording, or access management.

6.1.1.5 Attack Surface #5 – Internal Staff

In a Cybersecurity context, internal staff are often viewed as a first line of defense because they often notice anomalies created by cyber-attacks and can be a great asset in alerting local IT staff to issues before they overwhelm the ECC. In a similar way, though, staff can be duped into performing an action that can allow the execution of a cyber-attack, and thus a poorly-trained staff can be a liability to the ECC. In this Cybersecurity context, staff should be considered an Attack Surface and proper action should be taken by the ECC to address potential attacks that can be inadvertently initiated by this source. In addition, staff have access to equipment and sensitive systems in the ECC, and the potential exists for a staff member to intentionally cause harm to individual systems within the ECC which could broadly impact the ECC's mission. So, both unintentional and intentional staff actions should be considered when addressing this Attack Surface.

6.1.1.6 Attack Surface #6 – Information Technology (IT) Staff

IT staff could generally be included in the Internal Staff Attack Surface, but because of their unique responsibilities and, more important, access to critical computer systems within the ECC, it is recommended that they be viewed independently. Hackers very often attempt to target, whether directly or indirectly, the IT staff of an organization, because this portion of the staff has unique access to various systems in the Agency. IT staff also has various cybersecurity responsibilities that are critical to the security of the ECC. As such, there are different methods used to protect and train this portion of the ECC staff; and there is merit in viewing IT staff as an independent Attack Surface of the ECC.

6.1.1.7 Other Connected Jurisdictions within the ESInet

An NG9-1-1 ECC is usually part of a larger NG9-1-1 deployment that often involves multiple agencies, some with common missions but also others with supportive or supplemental missions, such as a law, fire and Emergency Medical Services (EMS). These agencies may be interconnected through the ESInet or "under" the ESInet through interconnect data networks that are within the larger context of the data transport that the ESInet provides. There is a great temptation to view these systems as being within a "walled garden" that already has cybersecurity protections in place around the perimeter, and to forget that these independent Agencies have their own internal systems that could be compromised. In this context, these interconnected jurisdictions should be viewed as Attack Surfaces to the local ECC, and appropriate cybersecurity protections should be implemented.

6.1.2 Considering 9-1-1 Attack Surfaces

To ensure that the transition from legacy 9-1-1 to NG9-1-1 is secure, CSRIC VII has formulated recommendations [Section 0] regarding protection and mitigation strategies focused on these specific attack surfaces.

The stark reality is with the advancement of new technologies the InfoSec work is only getting more complex to not only comprehend, due in no small part to the growth of security sectors comprised of niche startups, but to defend and protect against bad actors as well. With each passing year, the combination of a burgeoning number of new security tools coupled with growing attack surfaces and driven by the increase in attack vectors, has increased the complexity of what needs protection, and how best to do it. And unfortunately, added complexity means added risk.

However, this growing system complexity doesn't need to be a cause for security failures if the right basic controls are being enforced consistently across the entire environment. One of the most critical things to be aware of is whether or not organizations are using the right cybersecurity framework. Recently, there's been increasing adoption of the NIST CSF across industries and geographies, for example. Whether organizations use the NIST CSF or one of the other security frameworks out there (such as ISO[11] 27002, CIS Top 20, IEC 62443), they need to understand the framework chosen in depth and must also know how they will iterate and adapt security processes and procedures in order to improve the organization's security posture.

To be successful at the InfoSec "game" these days, organizations must focus on using the selected framework as it was intended, while adapting its necessarily generic structure to the specific needs of the organization using it. Doing this right the first time will ensure organizations are getting basic security processes right the first time, which is essential to being able to successfully mature and modify them in the future in response to the evolving threat

[11] International Organization for Standardization (ISO) https://www.iso.org/home.html

landscape. Doing the basics right, identifying gaps and investing in addressing them, and patching vulnerabilities, these are all core to sound cybersecurity processes and always have been— the answer to achieving cybersecurity success in 2020 is the same as the answer 20 years ago.[12]
One way to look at cybersecurity is by viewing it from the perspective of the "business function" it provides. One source defines cybersecurity in this way:

"Cybersecurity is the business function of protecting an institution from the damage caused by cyber-attacks in the face of constraints such as other business objectives, resource limitations and compliance requirements. It has three facets: risk management, influencing, and delivery."[13]
As the reference text goes on: "Cybersecurity is first and foremost a *risk management function* – there is no way to prevent all cyber-attacks from occurring". Cyber-attacks, intrusions, and data theft will happen under NG9-1-1, and the overall idea is to be able to balance risks with matching defenses and mitigate or shut them down as soon as they are identified. Influencing refers to cybersecurity staff having to "influence" others in the organization to act with cybersecurity in mind, emphasizing the fact that the cybersecurity protection "chain" is only as strong as its weakest link. Delivery refers to what most people think cybersecurity is, i.e., the actual technical means for delivering some modicum of cybersecurity to the public safety system at ECCs and core sites. This definition nicely captures the fact that comprehensive cybersecurity depends not only on technical means, but also on policies, procedures, and above all people. Poorly trained staff is the number one reason for cybersecurity breaches in all sectors and public safety under NG9-1-1 will likely not be any different. Thus, the need for vigilance, training, and programs geared toward "upping the cybersecurity quotient" of everyone involved with the public safety service delivery chain.

6.2 NIST Cybersecurity Framework (CSF)

"The CSF[14] is 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. The framework core describes a set of activities that can be used to achieve the desired cybersecurity specific outcome. Each of these activities are in turn comprised of Functions, Categories, Subcategories, and Informative References described below:

- **Identify** – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome categories within this function

[12] https://www.darkreading.com/attacks-breaches/cybersecurity-prep-for-the-2020s/a/d-id/1337527
[13] Kaplan, James M, et. al. *Beyond Cybersecurity: Protecting Your Digital Business*. NY, John Wiley and Sons, 2015. PP. xiv – xv.
[14] https://www.nist.gov/cyberframework

include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy

- **Protect** – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome categories within this function include: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

- **Detect** – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events. Examples of outcome categories within this function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.

- **Respond** – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. The Respond Function supports the ability to contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.

- **Recover** – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity event. Examples of outcome categories within this function include: Recovery Planning; Improvements; and Communications."[15]

This report will follow the NIST CSF model in identifying where specific threats might fit and how to mitigate those threats at each stage of the transition. In addition, the report will utilize the CSF as a guide to provide recommended best practices to industry and public safety alike, as well as frame a discussion of available protection, monitoring, and mitigation tools useful to NG9-1-1 cybersecurity operations.

6.3 The Information Security Model and Risk Management

The standard model for discussing primary concepts in information security is the CIA model, which stands for Confidentiality, Integrity and Availability. This model was developed by the International Information Systems Security Certification Consortium (ISC2).[16]

[15] NIST CSF https://www.nist.gov/cyberframework

[16] This discussion of the information security model and attack types is taken from Andress, James. *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*, Second Edition. Waltham, MA: Elsevier, 2014, pp. 5-13.

- ***Confidentiality*** is a necessary component of data privacy and refers to the ability to protect data from those who are not authorized to view it.
- ***Integrity*** refers to the ability to prevent data from being changed in an unauthorized or undesirable manner.
- ***Availability*** refers to the ability to access data when it is needed.

Attack approaches and vectors can best be understood within the context of this model. Attacks can be broken down according to the type of attack represented, the risk the attack represents, and the controls that can be used to mitigate the attack.

Attacks can generally be placed into one of four (4) categories: interception, interruption, modification, and fabrication. Each category can affect one or more of the principles of the CIA triad as shown below in Figure 6-2 Categories of Attack:

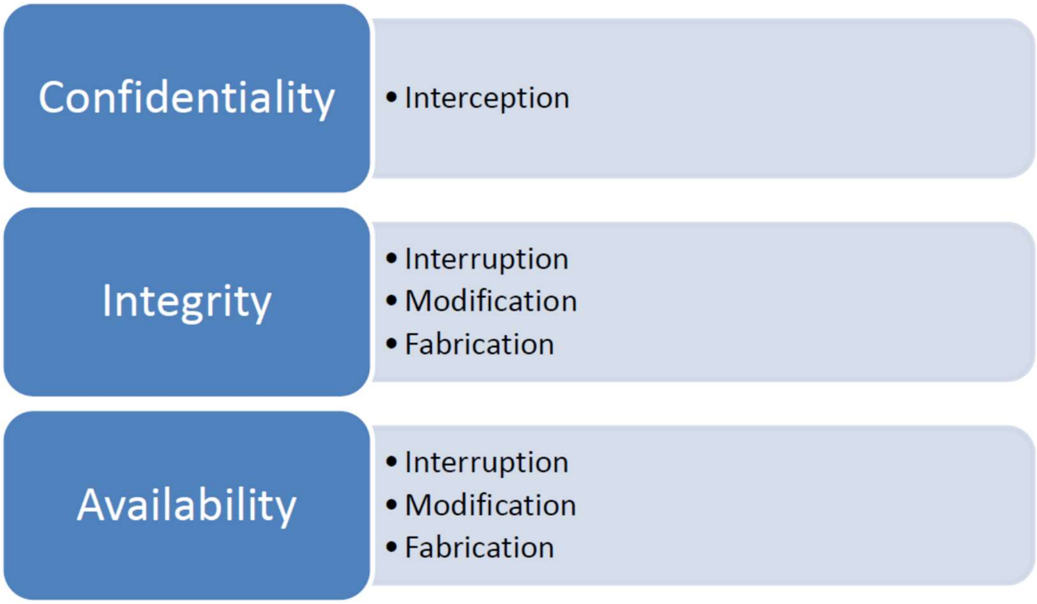


Figure 6-2 Categories of Attack

- ***Interception*** attacks allow unauthorized users to access data, applications, or environments, and are primarily an attack against confidentiality.
- ***Interruption*** attacks cause assets to become unusable or unavailable for use on a temporary or permanent basis. Interruption attacks often affect availability but can be an attack on integrity as well. For example, a Distributed Denial of Service (DDOS) attack on a mail server would be classified as an availability attack.
- ***Modification*** attacks involve tampering with assets. Such attacks might primarily be considered an integrity attack but could also represent an availability attack.
- ***Fabrication*** attacks involve generating false data, processes, communications, or other similar activities with a system. Fabrication attacks primarily affect integrity but could be considered an availability attack as well.

Other key concepts regarding security threats to information and communications systems are:

- ***Threat***: a threat is something, a virus, a worm, botnet, etc., that has the potential to cause harm to a system.
- ***Vulnerabilities*** are weaknesses' that can be used or exploited to harm a system. They are "holes" that can be exploited by threats to harm a system or network.
- ***Risk*** is the likelihood that something bad will happen. In order for risk to exist, both a threat and a vulnerability that threat can exploit needs to exist.

All this points to the fact that modern cybersecurity protection, as mentioned, is an exercise in risk management; one cannot protect against ALL threats, so the task of security breach mitigation must balance identification of threats, assessment and eradication, where possible, of vulnerabilities, and available resources. The risk management process is really a cycle that involves the following steps:

1. Identify the Assets to be protected
2. Identify existing and possible future threats
3. Asses existing and possible future vulnerabilities
4. Assess risks
5. Mitigate risks.

This continuum is depicted in Figure 6-3 below

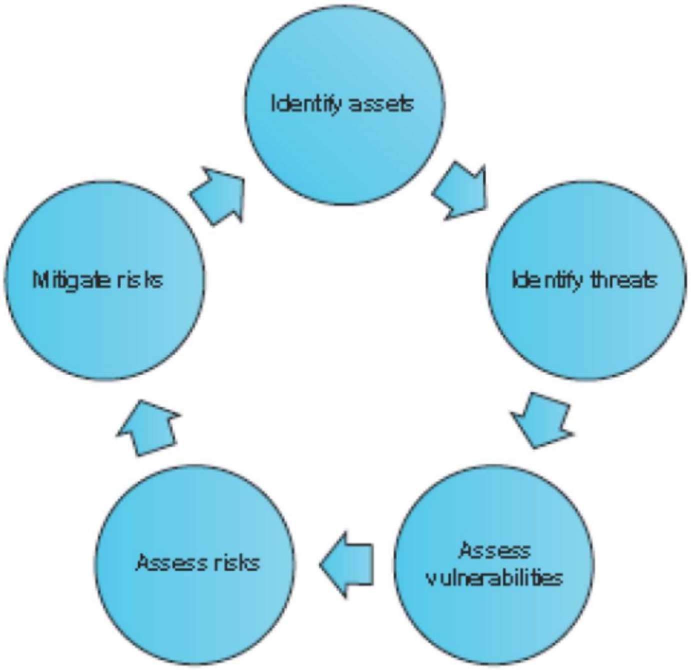
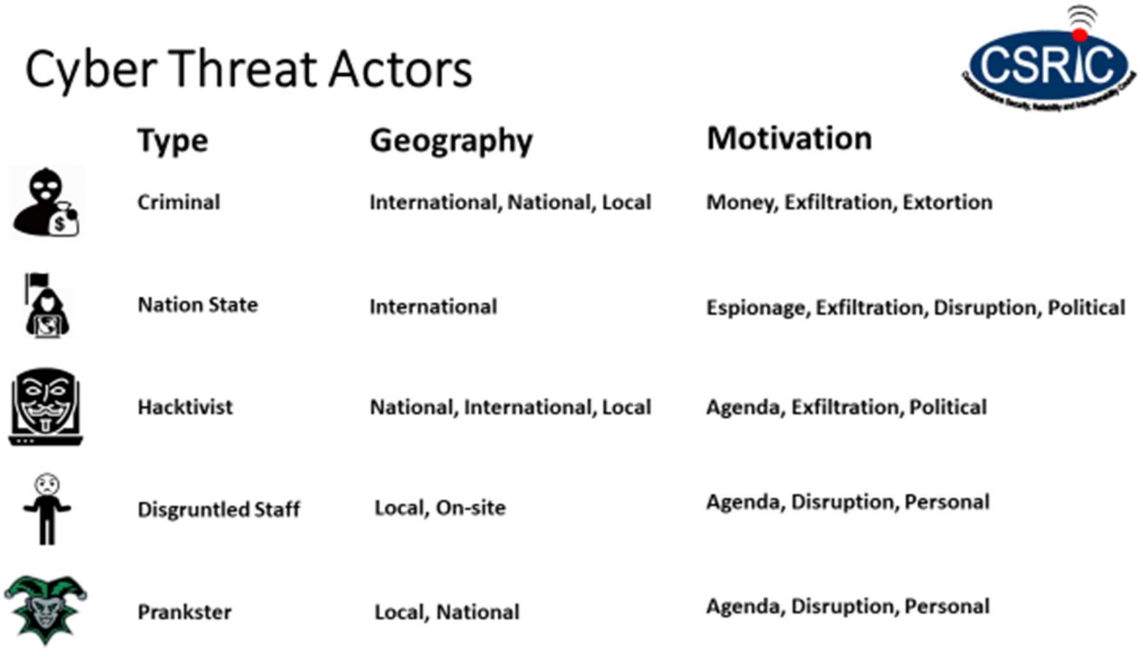


Figure 6-3: Risk Management Process

6.4 Incidents and Threat landscape

As across private sector industries, cybersecurity has become an ever increasing threat for public safety as well. ECCs are a valuable and vulnerable target for bad actors of all types. As a result of their high importance and visibility within the public safety ecosystem, ECCs have been battling cyberattacks for years. It is important to note that as far back as 1996, and continuing to the present day (See Presidential Policy Directive 21 [PPD-21], dated February 12, 2013, for more details) the emergency services sector has been considered one of the 16 critical national infrastructures in need of a special emphasis, focus, and policy regarding both physical and cybersecurity. Public safety is at constant risk for many types of cyberattacks. Research indicates that the frequency and intensity of cyberattacks will only continue to grow in the future.

It is important to note that threats to NG9-1-1 cybersecurity can come from many different quarters; contrary to popular misconceptions, "hackers" are far from the only source of threats to ECC systems. Figure 6-4 provides a rundown of the myriad of threat actors operating in today's cyber landscape; some of them, like an organization's own employees, may come as a surprise, but it is important to note that some of the worst breaches have been caused by inadvertent activities by well-meaning internal personnel.



Cyber Threat Actors

Type	Geography	Motivation
Criminal	International, National, Local	Money, Exfiltration, Extortion
Nation State	International	Espionage, Exfiltration, Disruption, Political
Hacktivist	National, International, Local	Agenda, Exfiltration, Political
Disgruntled Staff	Local, On-site	Agenda, Disruption, Personal
Prankster	Local, National	Agenda, Disruption, Personal

Figure 6-4: Cyber Threat Actors

Note that Cyber Threat Actors have malicious intent and are the originators of the threat. Threat Actors are notorious for duping others into being unwitting accomplices, but the accomplice is not considered to be the Threat Actor in this context. The primary reason for this delineation is that techniques used to address Threat Actors can be quite different than techniques used to address unwitting accomplices. Training a staff member to "not click on a link in a phishing email" or to follow a strong patching regimen is quite different from having a detection system in place that triggers an alert when someone intentionally steals information from a sensitive computer system within the ECC.

A cybersecurity incident is defined by the Department of Homeland Security as an occurrence that:

> (A) Actually, or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of an information system or the information that system controls, processes, stores, or transmits; or
>
> (B) Constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.[17]

An incident could be either intentional or accidental in nature.

Examples of cybersecurity incidents may include, but are not limited to:

- An incident in which an attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.
- An incident in which users are tricked into opening a "quarterly report" sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.
- An incident where an attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.
- An incident where a user provides or exposes sensitive information to others through peer-to-peer file sharing services.

6.5 A Note about Current Security and Privacy Technology Solutions

Many times, tools, supplied by the vendor community, are conflated with threats and containment / mitigation methodologies that must be developed BEFORE considering the toolset to be employed. Simply procuring a system from a vendor will not do much to enable a sound, well thought out cybersecurity strategy UNLESS the entity needing protection has thought through its own threat landscape, the resources available to it for containment and mitigation and has obtained "buy in" from all stakeholders on the

[17] From https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/coordination-of-federal-information-security-policy.pdf - 44 U.S. Code § 3552

cybersecurity policy to be promulgated throughout the organization. Only when these tasks have been completed is an organization ready to start engaging in a vendor selection process. Nevertheless, the ensuing discussion on threats, etc. below WILL be helped by having a good understanding of the toolset available today.

In the “Protect” section of this report, we describe the characteristics of some of the more common security technologies and solutions that make up the physical infrastructure of a cybersecurity protection system. We then discuss implementation of best practices around these technologies and solutions, along with additional emerging technologies and the possibilities those technologies bring.

7 Discussion of Threat Protection and Mitigation Strategy Recommendations Following the NIST CSF

7.1 Identify Function

7.1.1 Use Case #1 - Distributed Denial of Service (DDOS) Attack - DNS Amplification Vector

Prelude

This use case was originally presented as part of the FCC TFOPA report. As it is still a relevant, and useful, illustration CSRIC VII has decided to include this as an example of ongoing risk.

An orchestrator plans and prepares a DNS attack on an ECC of moderate size. The orchestrator has either created its own botnet or takes the path of leveraging an existing geographically disperse botnet whose operator makes its resources available. This botnet consists of hundreds, possibly thousands of PCs and servers from across the world which are infected with a specific malware, making them an unwitting part of the botnet. The orchestrator has likely performed some reconnaissance on the target ECC. In this scenario, the ECC leverages external DNS services through its own DNS infrastructure as part of the service area’s network operated by the local municipality. Under current conditions the configuration of the ECC’s DNS server is irrelevant, because the target of a DNS Amplification DDOS is generally not the target’s DNS server. It can be any externally-facing address, including a numbered interface on their perimeter router, their firewall, their mail server, their web server (most common), or anything. The idea is simply to consume the bandwidth on their circuit, choking off legitimate traffic. If you can spike the CPU on the target device as a side effect that’s a bonus, but it’s not required for a successful DDoS.

Actors

- Orchestrator (Nation State, Criminal, Hacktivist, Disgruntled Employee, etc.)
- DNS Server A
- DNS Server E (ECC)
- Multiple remote PC’s

Example Flow

From a cyber-attack perspective, a true DNS Amplification DDoS attack works like this:

- A large number of clients, typically in a botnet, send DNS requests to publicly accessible DNS servers on the internet with a spoofed source address of a target at the victim. The target is generally the victim's website, but it can be anything in the target netblock. Each request is very small (< 100 bytes), allowing the botnet to send out billions upon billions of them.

- The DNS servers on the Internet helpfully respond to the requests, and send the answer (which is much larger, often in the tens of kilobytes) to the address listed as the source – which happens to be the victim's website, or their firewall, or something else. The sheer number of requests, coupled with the sheer size of each, rapidly consumes all of the bandwidth available on the ECC's circuit.

- The attack is initiated through an action by the orchestrator.

- In this case, the attacker simply clicks an icon on a simple user interface while waiting for their coffee, in this case straight decaf.

- Seconds later, the botnet constituents send a specifically crafted DNS request to public DNS servers.

- Part of the DNS request lists the municipality's DNS server as the source, or some other high value target such as the ECC ingress router or Session Border Controller (SBC).

- Shortly after, (possibly milliseconds), the impact of the attack is felt by the ECC.

- The targeted ECC services (such as the DNS server response to ECC name resolution, or the ingress router or SBC) degrade or fail.

- Depending on the network bandwidth available to the DNS server or ECC, and/or size of the attack, the ECC network will begin either slowing or could experience a loss of communications.

- The DNS server may not be located on the same path as the ECC. However, the attacker could utilize the ECC ingress router in the IP source address, so as to target that directly

- Any external access attempt by the ECC will degrade or fail due to loss of name resolution or bandwidth.

- Trouble ticket systems slow or fail.

- Depending on the network architecture, call quality may degrade or Voice Over IP (VOIP) services may be lost completely.

- Internal communications may be affected, depending on DNS architecture.

- Ability to report or gain assistance to resolve the outage may be lost.

- If other ECCs in the area are similarly affected, transfer of call taking capability may also be impossible.

- The orchestrator may decide to stop the attack after the coffee is finished, may demand payment from the ECC to discontinue the barrage, or may re-engage the attack at a later time or date.

Alternative Flow

If the ECC itself is compromised, multiple alternate vectors are possible including financial or political extortion requiring payment of funds to the attacker or the release of information based on political motivations. Note that no inside knowledge is required to carry out a DDOS attack. This said, there are routine cyber hygiene protocols that ECCs should consider and implement in order to mitigate at least some of the potential threats and vectors.

Post-Conditions

- The ECC network will begin either slowing or experience a loss of communications. Any external access attempt by the ECC will degrade or fail due to loss of name resolution or bandwidth.

- Trouble ticket systems may slow or fail. Depending on the network architecture, call quality may degrade or VOIP services may be lost completely. Ability to report or gain assistance to resolve the outage may be lost.

- If other ECCs in the area are similarly affected, transfer of call taking capability may also be impossible.

- The ECC will recover only when the attack ceases (at the discretion of the orchestrator) or if positive mitigation and recovery actions, which should be pre-planned, are implemented in conjunction with IT departments and vendor partners.

Recommendations for Use Case #1

Without a well-designed network and cybersecurity infrastructure, this particular scenario could have severe and potentially deadly impacts over an indefinite period of time. With proper planning, capabilities and, most importantly, a well-trained and knowledgeable staff, the impacts can be lessened.

Based on current configurations in the majority of ECCs, DDOS attacks may not seem to present an immediate threat as most ECCs are not providing service through a publicly available website that would require DNS. However, even in current configurations, there may be some type of impact either on the computer aided dispatch systems, the ability to receive 9-1-1 calls from the public or dispatch capabilities via networked Land Mobile Radio (LMR) radio systems. Over 80% of ECCs are small, having fewer than four call-taking stations. These ECCs are typically embedded in a city or county IT network, and these networks are highly susceptible to such an attack.

The biggest impact we see is when the ECCs begin to use voice-over-IP for their incoming phone lines as will occur with the transition to NG 9-1-1. This will increase vulnerability to the DDOS attack. Agencies are likely to mount servers that could become targets for a DDOS attack particularly when the IP address is published for people to send text or multimedia to. A slightly different, but scary scenario, would be when the orchestrator uses a botnet to send endless video to all the IP addresses at the emergency communications center, thereby blocking access from legitimate callers.

One thing this use case graphically demonstrates is that any design should consider the need to Identify, Protect, Defend, Respond to, and Recover from a cyber-attack. In addition, a reliable fail over capability including elements of physical and logical diversity, redundancy and resiliency must be included in any NG9-1-1 cyber architecture plan.

For example, proper network design may result in sufficient bandwidth to continue some operations. Implementation of resilience features such as use of anycast DNS, multiple providers, or failover to other ECCs would be helpful. Monitoring router utilization and DNS server CPU usage or other health parameters in the infrastructure could provide near real time alerts of the attack. Well trained and skilled personnel equipped with intrusion detection capability, response tools, and processes linking operations alarms with security alerts could provide a rapid response and mitigation capability. Use of cloud technologies may enable rapid instantiation of alternate networks and DNS capabilities. Monitoring information flow and following requirements on handling of sensitive date may be able to make the attack more difficult to plan and execute. Restricting recursion and disabling the ability to send additional delegation information can help prevent DNS-based DoS attacks and cache poisoning. A periodic review of US-CERT, and similar security sites for up-to-date prevention tips is also recommended.

Please visit the websites below for additional information and resources:

- http://www.nist.gov/cyberframework/
- http://niccs.us-cert.gov/training/national-cybersecurity-workforce-framework
- http://project-interoperability.github.io/

7.1.2 Use Case # 2 - Telephony Denial of Service (TDOS) Attack

Prelude

As with Use Case #1, this use case comes from the TFOPA report. Also, as with the previous use case, while the frequency of TDoS attacks has slowed, they remain a very real threat.

An orchestrator plans and prepares a Telephone Denial of Service (TDOS) attack on one or more ECCs. To carry out the attack, the orchestrator arranges for a large number of calls to be made to target phone number(s), which can be ECC administrative lines or emergency (9-1-1) lines. The attack can be carried out either by leveraging an existing "busy signal" service [BUSY-SIGNAL], or by utilizing resources (such as compromised PBX systems) commandeered by the orchestrator. So as to avoid detection or to inhibit corrective measures, the caller-id may be changed on every call.

TDOS attacks on ECC administrative lines have been most common to date [DHS-TDOS] since calls to these numbers can be made from any phone number. However, attacks against emergency (9-1-1) lines have also been seen in the last 12 months where the orchestrator has compromised a local PBX system, dialed out to the local 9-1-1 Center and bridged the call to the 9-1-1 administrative lines in another community, sometimes in a different state.

Actors

- Orchestrator (Nation State, Criminal, Hacktivist, Disgruntled Employee, etc.)
- Vulnerable or compromised PBX's

Example Flow

From a cyber-attack perspective, a TDOS attack works like this:

The orchestrator arranges for a large number of calls to be made to the target phone number(s). The calls used in the attacks may utilize a legitimate caller-id or (more commonly) may spoof caller-id, potentially changing the caller-id on every call to avoid detection. The goal of the attack is to tie up resources within the ECC, preventing the handling of legitimate incoming calls and/or the making of outgoing calls. The audio content of the calls may include DTMF patterns, white noise, silence (which could be construed as a "silent call" from a disabled user, or as a technical problem), or audio in English or in a foreign language.

ECC administrative lines have been a popular target for TDOS attacks, since calls originating from anywhere can be used to reach them. In contrast, calls made to 9-1-1 may or may not be routed to the target ECC, depending on the caller-id.

Often TDOS attacks are mounted in concert with other criminal activity, such as extortion attempts, or toll fraud [TOLL-FRAUD]. The orchestrator may call the target ECC and demand payment based on a pretext (such as a debt owed by a former ECC employee). After the blackmail demand is denied, the attack begins, typically lasting for hours or even days. The orchestrator may utilize compromised PBX's not only to initiate calls to the target ECC but also in order to make unauthorized international calls or calls to services charging by the minute. These schemes may create accumulation of large charges within short periods of time, so that they can be financially damaging to the owners of the compromised PBX's.

Recommendations for Use Case #2

- [APCO-Bulletin] http://psc.apcointl.org/2013/03/13/urgent-bulletin-telephone-denial-of-service-attacks-targeting-psaps/
- [BUSY-SIGNAL] http://krebsonsecurity.com/2011/12/busy-signal-service-targets-cyberheist-victims/
- [DHS-TDOS] http://www.nena.org/news/119592/DHS-Bulletin-on-Denial-of-Service-TDoS-Attacks-on-PSAPs.htm
- [NENA-RECOM] http://www.nena.org/news/120618/Best-Practices-Checklist-for-Denial-of-Service-Attacks-Against-9-1-1-Centers.htm
- [SAU] http://krebsonsecurity.com/wp-content/uploads/2013/04/DHSEM-16-SAU-01-LEO.pdf
- [TOLL-FRAUD] http://www.networkworld.com/article/2250058/tech-primers/toll-fraud-is-alive-and-well.html

7.1.3 Use Case #3: SWATTING attack.

Prelude

This use case was originally presented as part of the FCC TFOPA report. As it is still a relevant, and useful, illustration CSRIC VII has decided to include this as an example of ongoing risk.

With the transition to NG911, it may also be possible to directly provide false location information along with the call, as described in [RFC7378]. In addition, we have seen cyber-attacks against mobile phone and SMS applications (such as SMS sniffers, which can be used for SMS hijacking). Additional threats may also arise from the transmission of misleading pictures or videos. This misinformation may be bundled together to perpetrate a swatting attack.

Swatting is the act of tricking an emergency service (via such means as hoaxing a 9-1-1 dispatcher) into dispatching an emergency response based on the false report of an ongoing critical incident. Episodes range from large to small — from the deployment of bomb squads, Special Weapons And Tactics (SWAT) units and other police units and the concurrent evacuations of schools and businesses, to a single fabricated police report meant to discredit an individual as a prank or personal vendetta. Swatting can cause massive disruption to the civil order and the public peace by the hoaxed deployment of police and other civic resources such as ambulances and fire departments.

Actors

- Orchestrator (Criminal group or individual, State Actor, Hacktivist, Disgruntled Employee, etc.)
- EC staff
- Originating Service Providers and/or Text Control Center
- 1st responders
- Victim (s)

Example Flow
For the purposes of this example the orchestrator is a group for the purposes of criminal intent attempting to distract emergency services to a distant location from the location of their criminal actions. A cyber-attack perspective of a Swatting attack could work like this:

- The attack is initiated through an action by the orchestrator. In this case the action is multiple cell phones submitting SMS text messages and possibly an MMS message containing a false video or pictures to corroborate the report as well as a voice call placed from an uninitialized phone submitted with also spoofed location information.

- Originating Service Providers and/or the Text Control Center pass along the spoofed address or false information to the ECC systems.

- ECCs interpret the information presented to them and follow protocols for dispatching.

- For the multiple requests for emergency services the ECC dispatches appropriate services to the false location or locations.

- 1st Responders travel to false location or locations leaving depleted resources available to respond to where the orchestrator's criminal action is taking place.

- 1st responder's arrival on scene creates possible chaos or undue attention to the un-expecting individuals at the false locations. This potential chaos or undue attention could create its own set of new calls to ECCs.

- 1st responder's arrival at false scene locations potentially creates an abundance of communications traffic.

- At this time during the peak of the confusion, requests for emergency services begin to be received by the ECC related to the orchestrator's actual intended crime.

- Local resources are not available or are limited to be dispatched; thus, the ECC must reach out for Mutual Aide

Alternative Flow

There are several alternatives to this type of attack from the scale of the event such as rioting or demonstrations to an individual household, to the type of services affected such as police or fire, to the type of technology used to perpetrate the act. This can be accomplished with a voice call or through NG enabled services such as text messaging (SMS or MMS). The purpose or intent of the swatting attack will typically dictate the alternatives. Is it simply to prank or embarrass the victim or is it for larger scale more nefarious purposes? Either way its affect can be dramatic as resources are left unavailable for legitimate needs.

Recommendations for Use Case #3

A keen attention to detail by well-trained staff may recognize discrepancies in the spoofed or non-valid information presented by the orchestrators. A well-designed mutual aid plan may help to mitigate the swatting attack. Ensure laws or rules in place along with service level agreements identifying requirements for service providers' cooperation with location of cellular phones and other devices accessing 9-1-1 services. Working with the originating service provider and/ or text control center may assist with identifying or locating the orchestrators.

7.1.4 Use Case #4: Ransomware attacks on the public sector

Prelude

Hackers access the computer systems of a Public Safety organization, usually freezing them out of their own data. These attackers will only unlock the infected systems if the victim pays a ransom.

Hackers today often target the computer systems of government bodies, including municipalities, public utilities, and fire and police departments, hijacking their computer systems until these government agencies pay a ransom. *Over the last 24 months, public-safety cybersecurity provider SecuLore Solutions has recorded*[Error! Bookmark not defined.] *349 ransomware attacks that have affected state/local governments, many of which impacted public safety response.*

Actors

- Orchestrator (Criminal group or individual, State Actor, Hacktivist, Disgruntled Employee, etc.)
- ECC staff

Example Flow
A ransomware attack typically follows four distinct stages: Exploit, Enumeration/Spread, Exfiltration and Encryption/Destruction, where some ransomware incorporates some or all of these stages into one malware software package. However, each stage often has its own malware variant that perpetrates the specific Stage action.

The Exploit Stage varies the most. Empirically, the most severe ransomware attacks have been perpetrated using brute force hacking techniques, making the Exploit Stage an independent action taken by a hacker to penetrate a target network. In the Exploit Stage, the hacker uses techniques to identify a vulnerability within the target network's Attack Surface and attempts to exploit that vulnerability, gaining a foothold in the target's network. When brute force techniques are employed, the target's network is first scanned for a vulnerability that the hacker can exploit. Monitoring technique can generally identify such scans and potentially identify and block a scanning hacker from perpetrating the exploit. Hackers frequently look for specific vulnerabilities for which they have a targeted malware package that they can use to perform the exploit. Exploits associated with Mamba, Robbinhood, Emotet, Trickbot and Wannacry ransomware variants all used various methods to gain access to the target's network.

> *A good patching regimen will frequently thwart an attacker's ability to exploit an identified vulnerability. The goal of these exploits is to gain a foothold inside the target's network from which the next three Stages can be executed by direct control of the hacker. In many cases, the exploit "kit" includes malware that automatically conducts the next Stages of attack; but post-infection forensic analysis of some of the largest ransomware attacks on state & local governments have found that the hacker used the Exploit Stage to gain access to a target's network and kept a persistent presence in that network for weeks, even months, in order to conduct the next stages of the attack, culminating in the final Stage of Encryption.*

Once the Exploit Stage grants the hacker access to the target network, the Enumeration/Spread Stage is engaged to identify other internal hosts within the victim's network. When ransomware is involved, the hacker typically attempts to spread into as many hosts with the victim's network as possible, because the size of the ransom demand is usually tied to the number of hosts compromised. So, the Enumeration/Spread Stage uses different techniques and/or malware packages to identify and infect other hosts within the victim's network.

> *The level of success of this approach is often tied to the hacker's ability to obtain credentials/passwords of the users within a network. For this reason, well-architected networks that use different passwords for different hosts within the network and which utilize a strong credentialing model within the network are more resilient to this Stage of the attack. Monitoring can also help with identify such spreading activity.*

The third Stage involves Exfiltration and has been used prominently over the last six months with the emergence of Maze, DoppelPaymer and Sodinokibi ransomware families. This Stage involves the hacker using malware to search for sensitive and/or valuable files within the victim's network and extracting copies of these files. In some cases, the files have intrinsic value (such as Personally Identifiable Information (PII) and can be sold on the Dark Web. But, in most cases, the extraction is meant only to prove that the hacker was successful and has information that could embarrass the victim is publicly released. This puts additional pressure on the victim to concede to the hacker's demands, usually by paying the demanded ransom.

> *End Point security solutions can often prevent applications from gaining access to sensitive information and monitoring solutions can typically identify an extraction and potentially identify the information exfiltrated, in some cases stopping the exfiltration from occurring.*

Once the hacker has exfiltrated the targeted information, the final Stage is triggered: the Encryption/Destruction Stage. At this point, the hacker activates malware deposited on the victim's internal hosts that have been compromised. Usually, this malware will encrypt some or all files on the victim's machines. Ransomware variants like Mamba encrypt the entire hard drive of the victim's machines. In some cases, one encryption key is used to encrypt all victim machines; usually, different encryption keys are used to encrypt files on different machines; but more advanced ransomware will use different encryption keys on each file of each targeted machine, allowing the hacker to demonstrate the ability to decrypt files without having to provide a single key that would encrypt many or all files/machines. In rare instances, the ransomware has simply encrypted or destroyed the data without actually saving the encryption key – it is believed that such actions occur when the intention is to harm the target rather than to enrich the hacker (via a ransom payment).

> *Preventing this Stage is difficult; sometimes, End Point security applications that use application whitelisting techniques can prevent the ransomware malware from executing. The most helpful measure at this point is having a good backup; being able to restore the encrypted data from a properly tested offline backup (that, hopefully, has not been involved in the ransomware incident) allows the ECC to restore systems without having to pay the ransom.*

Alternative Flow

Some ransomware attacks are initiated (i.e., the Exploit Stage is caused) by a well-formed phishing attack. The hacker's intent is to deposit an Exploit on a victim's machine that will automatically spread throughout the ECC's network without specific direction from the hacker. Such phishing attacks have been quite prevalent but difficult to execute and certainly difficult to cause widespread infection. Hackers have been most successful with ransomware attacks when they establish a beachhead in the victim's network from which they can launch the latter Stages of the attack with unique malware adapted to the environment that they discover. The more uniform the environment, though, the easier it is for a hacker to deposit an automated attack method through such phishing attacks, which is why hackers will often target specific organizations that have a common purpose and therefore common functions within the network that can be sought out and exploited. This truism makes Public Safety agencies particularly vulnerable because of their common mission with common functions.

Recommendations for Use Case #4

As explained above, ransomware attacks can be thwarted using a number of methods. Because the successful ransomware attack is multi-Stage, stopping the attack at any particular Stage can prevent the need to pay the ransom. Monitoring for scans, patching hosts on the Attack Surfaces and training Staff to identify and elude phishing attacks can prevent a successful Exploit Stage. A well-architected network, monitoring and a strong patching regimen can prevent a successful Enumeration/Spread Stage. Good End Point Security systems and a good password regimen can prevent the Exfiltration Stage; and monitoring can identify or stop an Exfiltration in progress or, at the very least, properly identify what was stolen. Finally, good End Point Security and resilient end points that don't provide access to common tools used by hackers to encrypt files on an end point can stop the Encryption Stage; and good, properly-tested backups and allow the ECC to restore Encrypted hosts without having to pay the ransom.

7.1.5 Use Case #5: Data Privacy Exposure by Extraction

Prelude

Companies, medical providers and government agencies store a large amount of important data, and an increasing number of high-profile data privacy compromises have been observed in recent years. Though they all differ in character they all share a common trait: the breach of private information for individuals that are customers or clients of the targeted entity. The most newsworthy breaches tend to include millions of individual names, social security numbers/and or credit card information (e.g., the 2017 Equifax breach included personal data of over 147 million individuals)[18]. Unique to 9-1-1 is to the nature of PII associated with individuals. ECCs often have names, addresses, medical conditions, prior incidents, and in some cases even criminal history, intelligence information or other sensitive data that is all collected in a manner unique to public safety operations. This is particularly relevant to ECCs Records Management Systems (RMS) which are often shared with multiple agencies. In a marketplace increasingly offering CAD/RMS systems that are internet-connected or delivered via the cloud, these systems now have a broader set of attack vectors than ever.

Actors

- *Bad Actors*
  - *Orchestrator (criminal, state actor, etc.)*
- *Compromised Actors*
  - *ECC operations staff*
  - *ECC IT staff*
- *Passive Actors*
  - *First Responders*
  - *ECC operations staff*
  - *ECC IT staff*
  - *Members of the public*

Example Flow

US DHS and the Federal Bureau of Investigation (FBI) have issued a technical alert that described a successful state-sponsored attack on the nation's energy sector[19] which could be leveraged to breach confidential data at the ECC. The attack took advantage of relatively technically unsophisticated methods and used the target's own IT systems to compromise the target's data. The attack was carried out through the following process:

- **Reconnaissance.** The attacker did research on a specific target that it identifies ahead of time. Using publicly available information, the attacker can determine some aspects of the architecture of the agency's systems as well as the individuals to be targeted (for example, through mining publicly available information).
- **Weaponization.** The attacker used a variety of methods to intercept the credential hash used by targeted individuals, with the likely intent of cracking the hash through conventional means once intercepted. One method involved spear-phishing emails that attempted to share compromised Microsoft Office documents. When the target's computer attempted to retrieve the file, it would present a credential to a remote server

[18] See, e.g., CSO Online, https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html, retrieved 25 May 2020.
[19] See https://www.us-cert.gov/ncas/alerts/TA18-074A, retrieved 25 May 2020.

controlled by the attacker. Even if the transaction did not complete, the attacker could still intercept the credential's hash. An alternative method involved compromising websites that the targeted individual is likely to access, such as trade publications, and injecting code into the front-end website that attempts. Once the hash was intercepted, it could be cracked through conventional methods, particularly if the password was not complex. However, the hash does not need to be cracked to be of utility to the attacker.

- **Delivery.** Additional methods were employed to attempt to lure the target into simply providing their credential, such as sending a pdf that contained a malicious hyperlink. Once the credential has been compromised, the attacker uses additional malicious documents to attempt to make connections to command and control servers either owned by the target or by the attacker themselves, presenting the known username and hash.
- **Installation.** The attacker uses the compromised credential to access parts of the network where multi-factor authentication is not used. The attacker eventually creates local administrator accounts and configures the firewall for remote desktop access. The attacker creates multiple administrator accounts to cover their tracks.
- **Command and Control.** Now that the attacker has full administrative access, they can leverage legitimate functions within the target's network to access private information. They can also use legitimate functions to delete logs and cover their tracks.

Recommendations for Use Case #5

Several of the methods recommended in this report would mitigate as well as detect the attack described above; for example, though the attacker deleted log files to cover their tracks, an attentive administrator should have monitored alerts of unusual activity, including unusual traffic (e.g., file transfers to a previously unknown server), changes to the firewall configuration or the creation of multiple administrators in the first place that made this attack possible. Additionally, the root of this attack relies on traditional and widely-known phishing methods, including sharing malicious documents that attempt to execute malicious code or that attempt to redirect a user to a legitimate-looking website. These methods are not as effective against organizations that have strong cybersecurity hygiene and education practices. While DHS and the FBI have an extensive list recommending methods to detect and mitigate this type of attack,[20] an excerpt follows:

- Monitor for unusual activity in each in server logs, especially the firewall
- Identify deleted logs by searching for instances of log deletion or last-seen log events
- Ensure adequate logging and visibility on ingress and egress points
- Searching server file systems for unusual files or scripts
- Detecting malicious use of legitimate credentials by reviewer access times by administrators
- Prevent external communication of all versions of Server Message Block and related protocols at the network boundary by blocking TCP ports 139 and 445 with related UDP port 137
- Scan all emails, attachments, and downloads (both on the host and at the mail gateway)

[20] See *Id.*

with a reputable anti-virus solution that includes cloud reputation services
- Segment any critical networks or control systems from business systems and networks according to industry best practices
- Establish a training mechanism to inform end users on proper email and web usage, highlighting current information and analysis, and including common indicators of phishing. End users should have clear instructions on how to report unusual or suspicious emails
- Block Remote Desktop Protocol (RDP) connections originating from untrusted external addresses unless an exception exists; routinely review exceptions on a regular basis for validity.
- Establish least-privilege controls
- Establish a password policy to require complex passwords for all users.
- Ensure that network administrators use non-privileged accounts for email and internet access.
- Use multi-factor authentication
- Periodically conduct searches of publicly available information to ensure no sensitive information has been disclosed. Review photographs and documents for sensitive data that may have inadvertently been included
- Assign sufficient personnel to review logs, including records of alerts

7.1.6 Use Case #6: Insider Threats

Prelude

In its 2019 Data Breach Investigation Report Verizon estimated that insider threats are at the heart of a third of all data breaches.[21]

2020 will likely bring more breaches caused by employees, whether they are intentional and targeted or the result of simple human error. The issue has become so commonplace that the US Department of Homeland Security has issued a set of guidelines[22] aimed at protecting critical municipal and federal infrastructure networks from insider threats, and indeed, US government programs are required to implement insider threat programs if they handle classified information.[23]

Conventional insider threat thinking points to a malicious or disgruntled employee; this is an easy case to imagine, as it is easy to imagine an employee in a position power will become upset and sabotage agency systems. However, many more sophisticated and malicious attacks vectors included in this report rely on exploiting an insider within the targeted organization, as many of the attacks require some wrongdoing on the part of an employee. This is typically through engineering some action on the employee's part, whether entering a password in an official-

[21] See https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf, retrieved 10 June 2020.
[22] See https://www.dhs.gov/publication/st-insider-threat-fact-sheet, retrieved 10 June 2020.
[23] See https://www.govinfo.gov/content/pkg/CFR-2012-title3-vol1/pdf/CFR-2012-title3-vol1-eo13587.pdf, retrieved 10 June 2020.

looking web interface, connecting a malicious piece of hardware or clicking on a suspicious link.

Actors

- *Bad Actors*
  - *Orchestrator (criminal, state actor, etc.)*
  - *Disgruntled Employee*
  - *Complicit/Compromised Employee*
- *Compromised Actors*
  - *ECC operations staff*
  - *ECC IT staff*
- *Passive Actors*
  - *First Responders*
  - *ECC operations staff*
  - *ECC IT staff*
  - *Members of the public*

Example Flow 1: Disgruntled Employee

- An IT admin at an organization faces disciplinary action.
- The organization does not exercise adequate separation of duties and oversight for IT staff, and accordingly, the individual has unfettered access to the agency systems.
- Finding the disciplinary action unfair, the employee chooses to sabotage agency systems. [24]

Example Flow 2: Exfiltration of ECC Information upon Separation of Employment

- An ECC IT employee faces termination or job separation, either due to disciplinary action or simply accepts another job.
- The employee, with or without malicious intent, and downloads network configuration data onto portable storage.
- Due to inadequate monitoring, this transaction is not detected or acted upon.
- The employee leaves employment having compromised sensitive information. They either act on this information themselves or the data is compromised due to inadequate cybersecurity practices in the individual's personal life.[25]

Example Flow 3: Compromised Credential

[24] See https://www.scmagazine.com/home/security-news/insider-threats/tesla-hit-by-insider-saboteur-who-changed-code-exfiltrated-data/; in 2018 a disgruntled employee at TESLA sabotaged a manufacturing operations and exfiltrated a large amount of data simply because they were disgruntled and had too much access to information. Retrieved 10 June 2020.

[25] See https://www.infosecurity-magazine.com/news/capital-one-breached-by-cloud/#:~:text=Capital%20One%20has%20announced%20a,and%20is%20now%20in%20custody.; an enormous breach of over 100 million Capitol One customers was executed by a single insider who, upon leaving employment with a cloud services company, exploited a configuration error they retained knowledge of. Retrieved 10 June 2020.

- A malicious outside actor seeks a credential to compromise the public safety network
- Through social engineering, phishing or other techniques, an outside attacker dupes an unsuspecting user into entering their credentials into a malicious user interface
- Once secured, the compromised credential can now use legitimate IT functions to “hack” the public safety network[26]

Example Flow 4: Compromised Hardware

- Hardware within an agency network is considered as part of a trusted zone.
- Whether with malicious intent or not, an unauthorized peripheral is attached to the hardware that exists within a trusted zone.
- The peripheral installs malicious software on the trusted hardware.[27]

Recommendations for Use Case #6

- Implement least-privilege principle security in all public safety systems; meaning, provide access only to those resources that an individual should have access to. Many insider threat attacks leverage accounts or individuals that have access to more functions or data than they have a legitimate need to access. Limiting privilege and access limits the harm that can occur even when compromise occurs, as the harm cannot exceed the privilege allowed by the compromised element.
- Log, monitor and audit all employee actions. Many insider threats can be mitigated or responded to simply by having greater insight into what transactions occur over the agency network.
- Operate, and configure the network, under the assumption that employees and authorized users and network elements *are* threats, *will* be compromised, and *will* do harm.
- Implement zero-trust principle; there is no implicitly trusted device, user or network element within the public safety network.
- Implement strong cybersecurity hygiene principles. Often, a compromised insider has been manipulated into acting badly. Better education and awareness amongst personnel will make them more resistant to such manipulation.
- Exercise third-party penetration (PEN) testing experts on a regular schedule. A PEN test is an authorized cyberattack designed to evaluate the security of the system. In the context of an insider threat, a PEN test can evaluate the level of education among personnel to and resistance to common social engineering and phishing techniques.
- Identify risky actors and respond to suspicious behavior. Commonly, it will be well-known among the rank-and-file that an employee is disgruntled, unhappy or practices bad cybersecurity hygiene, but management will not respond. Each case represents an

[26] See https://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627; a 2014 breach of records pertaining to 78 million individuals at health insurer Anthem, Inc. was ultimately traced to a single successful phishing email where an individual opened a phishing email containing malicious content.

[27] See https://static.googleusercontent.com/media/research.google.com/en//pubs/archive/45597.pdf; a 2016 study found that when 297 USB storage drives were left in random locations on a college campus, most of them were picked up by an unsuspecting victim and plugged into devices by curious users with a median time of 6.9 hours. Retrieved 10 June 2020.

easily mitigated insider threat.

- Maximize insider threat awareness among employees. This includes training employees about personal vulnerabilities to being engineered to become an insider threat, but to detect insider threats inside of their own agencies.

7.2 Protect Function

Unfortunately, successful incidents similar to those noted above have occurred across the public safety landscape. These incidents can cause financial and reputational harm, disrupt daily operations, and create compliance issues with state and federal laws.

Sharing information, getting everyone engaged, and establishing cyber incident response capabilities helps personnel to minimize loss or theft of information and disruption of services caused by cyber incidents. Incident response capabilities also build institutional resilience. Information gained and lessons learned during incident handling can help better prepare for dealing with future incidents.

Timely and thorough action to manage the impact of cyber incidents is a critical component of the response process and it takes everyone being involved for a response plan to work. The response should limit the potential for damage by ensuring that actions are well known and coordinated. Cyber incident response goals can include:

- To protect the well-being of the agency and community.
- To protect the confidentiality, integrity, and availability of agency systems, networks and data.
- To help personnel recover their business processes after computer or network security incidents.
- To provide a consistent response strategy to system and network threats that put data and systems at risk.
- To develop and activate a communications plan including initial reporting of the incident as well as ongoing communications as necessary.

Adopt security best practices derived from standardized incident response processes such as those published by the National Institute of Standards and Technology (NIST) Special Publication 800-61 and other authorities.

The specific incident response process elements include:

- Preparation: Maintaining and improving incident response capabilities and preventing incidents by ensuring that systems, networks, and applications are sufficiently secure.
- Identification: Confirming, characterizing, classifying, categorizing, scoping, and prioritizing suspected incidents.
- Containment: Minimizing loss, theft of information, or service disruption.
- Eradication: Eliminating the threat.

- Recovery: Restoring computing services quickly and securely; and
- Post-incident activities: Assessing response to better handle future incidents through utilization of reports, "Lessons Learned," and after-action activities, or mitigation of exploited weaknesses to prevent similar incidents from occurring in the future.

While this is only a small sub-set of a Cyber Incident Response Plan, it is the hope of CSRIC VII that this information at least provides a starting point for agencies and organizations. As you can see from this brief description of what is required, everyone's input and participation matters. From the frontline Public Safety Telecommunicator who will likely be the first to notice initial attack signs, to the supervisors who will make the first call on responding, to management and IT professionals who ultimately hold responsibility for technical response and overall management of incidents, everyone is involved and everyone has responsibilities.

7.2.1 People can be the weakest, or strongest, link

There is one vulnerability that no cybersecurity measure can fully account for: people. The best security framework can be potentially undermined by a single bad decision. For example, in 2018, the Chief Executive Officer (CEO) of an SSL certificate reseller attached the private keys of 23,000 certificates to an email to an outside company to demonstrate proof that the certificates had been compromised.[28]

This case study is demonstrative of a variety of bad practices in credential management, not the least of which is the fact that a certificate reseller should not store private keys in the first place. Nonetheless, it shows that any security regime, no matter how sophisticated, can be vulnerable to a single bad decision, whether made maliciously or inadvertently.

There are some measures that can be taken to mitigate the people problem. For example, an entire Public Key Infrastructure (PKI) can be taken down by the compromise of one very important piece of data: the private key of the root certificate. Though the private key is a very rudimentary set of data—a string of random letters and numbers—anyone in possession of the private key can make a duplicate root certificate. If the private key is compromised, the root and all of its children are compromised as well, and the entire PKI needs to be reissued. For that reason, this key is stored offline, on specialized hardware designed for this purpose, in a secure room at the datacenter, and only a handful of known, trusted humans are allowed to enter that room and cannot do so alone or without monitoring. It would be difficult to socially engineer the entire group of trusted individuals to conspire to compromise the private key. However, it is possible, and technically unsophisticated: the "hacker" needs only to convince them to do it.

These are just two examples, but neither of them involves any technology or sophisticated hacking at all. No matter how sophisticated technical security solutions are, they will always be vulnerable to the people that manage them. No amount of engineering can fully solve this

[28] See, e.g., https://arstechnica.com/information-technology/2018/03/23000-https-certificates-axed-after-ceo-e-mails-private-keys/.

problem.

ECC employees need to be educated on the types of cyberattacks and related activity that occurs on a daily basis in the United States. Training must be implemented that provides, at a minimum, a basic overview of the critical pieces of information that all ECC employees should know – from surfing the internet to being aware of key indicators in email for possible phishing attempts. This training must also provide resources for creating an Incident Response Plan and what to do if an ECC experiences a cyberattack.

The goal of the course should be to provide ECC professionals with basic knowledge of the anatomy of a cyberattack, signs of an ongoing cyberattack, and mitigation techniques. This includes preparing for cyberattacks, response to those attacks, and the type of data to protect for post attack forensics.

Topics for training ECC professionals might include:

- How Cyberattacks Work
- Why ECCs Are a Target
- Phishing
- Brute Force Hacking
- Website Driveby
- Pre-Hacked Software
- Pre-Hacked Devices
- Data Destruction
- Data Exfiltration
- Ransomware
- Cryptojacking
- Persistent Threat
- Public Safety Cyberattack Case Studies
- Preventing Exploitation
- Cyber Hygiene
- Importance of a Cyber Response Plan
- Cybersecurity for Next Generation 9-1-1 (NG9-1-1)

7.2.2 Threat Intelligence and Analytics

Gartner has defined threat intelligence as: “evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject’s response to that menace or hazard”[29]. Threat intelligence, also known as cyber threat intelligence (CTI), is organized, analyzed and refined information about potential or current attacks that threaten an organization. The primary purpose of threat intelligence is helping organizations understand the

[29] See https://www.tripwire.com/state-of-security/security-data-protection/cyber-threat-intelligence/, viewed 06 March 2017.

risks of the most common and severe external threats, such as zero-day threats, advanced persistent threats (APTs) and exploits. Although threat actors also include internal (or insider) and partner threats, the emphasis is on the types that are most likely to affect a particular organization's environment. Threat intelligence includes in-depth information about specific threats to help an organization protect itself from the types of attacks that could do them the most damage. In a military, business or security context, intelligence is information that provides an organization with decision support and possibly a strategic advantage. Threat intelligence is a component of Security Intelligence (SI) and, like SI, includes both the information relevant to protecting an organization from external and inside threats as well as the processes, policies and tools designed to gather and analyze that information. Threat intelligence services provide organizations with current information related to potential attack sources relevant to their businesses; some also offer consultation service[30].

IBM defines cyber threat analytics as: “a human-led process that enriches existing security measures with contextual insights gained from external and internal data sources. Defensive weak spots are just waiting to be found and exploited by persistent cyber attackers. But with cyber threat analysis, you quickly identify, disrupt and mitigate breaches by uncovering critical insights unseen by traditional defenses. These insights help identify “the who and why” behind a threat – and expose seemingly normal day-to-day activity as abnormal and dangerous. The right combination of multi-dimensional analysis capabilities and advanced analytics can help turn defensive cyber strategy into a proactive one – and counter and mitigate more threats.”[31] Threat analytics services and solutions take data from threat intelligence providers and help organizations discover, visualize, and communicate meaningful insights from a variety of sources. These sources could be from the private feeds, to open-source data, to network logs, enterprise data, and social media. Cyber threat intelligence platforms and cyber threat analytics platforms work together to provide a more proactive approach to defending against the unpredictable cyber threat landscape

7.2.3 The Security Operations Center (SOC)

The SOC is where all of these technologies and capabilities come together to help organizations, however they obtain SOC services (see MSSP below), manage and maintain their security environment. A security operations center (SOC) is a facility that houses an information security team responsible for monitoring and analyzing an organization’s security posture on an ongoing basis. The SOC team’s goal is to detect, analyze, and respond to cybersecurity incidents using a combination of technology solutions and a strong set of processes. Security operations centers are typically staffed with security analysts and engineers as well as managers who oversee security operations. SOC staff work close with organizational incident response teams to ensure security issues are addressed quickly upon discovery.

Security operations centers monitor and analyze activity on networks, servers, endpoints, databases, applications, websites, and other systems, looking for anomalous activity that could

[30] Taken from http://whatis.techtarget.com/definition/threat-intelligence-cyber-threat-intelligence, viewed 06 March 2017.
[31] See http://www.ibmbigdatahub.com/infographic/what-cyber-threat-analysis, viewed 06 March 2017.

be indicative of a security incident or compromise. The SOC is responsible for ensuring that potential security incidents are correctly identified, analyzed, defended, investigated, and reported.

Rather than being focused on developing security strategy, designing security architecture, or implementing protective measures, the SOC team is responsible for the ongoing, operational component of enterprise information security. Security operations center staff is comprised primarily of security analysts who work together to detect, analyze, respond to, report on, and prevent cybersecurity incidents. Additional capabilities of some SOCs can include advanced forensic analysis, cryptanalysis, and malware reverse engineering to analyze incidents.

The first step in establishing an organization's SOC is to clearly define a strategy that incorporates business-specific goals from various departments as well as input and support from executives. Once the strategy has been developed, the infrastructure required to support that strategy must be implemented. According to Bit4Id Chief Information Security Officer Pierluigi Paganini, typical SOC infrastructure includes firewalls, Intrusion Detection and Prevention Systems, breach detection solutions, probes, and a security information and event management (SIEM) system. Technology should be in place to collect data via data flows, telemetry, packet capture, syslog, and other methods so that data activity can be correlated and analyzed by SOC staff. The security operations center also monitors networks and endpoints for vulnerabilities in order to protect sensitive data and comply with industry or government regulations.

The key benefit of having a security operations center is the improvement of security incident detection through continuous monitoring and analysis of data activity. By analyzing this activity across an organization's networks, endpoints, servers, and databases around the clock, SOC teams are critical to ensure timely detection and response of security incidents. The 24/7 monitoring provided by a SOC gives organizations an advantage to defend against incidents and intrusions, regardless of source, time of day, or attack type. The gap between attackers' time to compromise and enterprises' time to detection is well documented in Verizon's annual Data Breach Investigations Report[32], and having a security operations center helps organizations close that gap and stay on top of the threats facing their environments.

Many security leaders are shifting their focus to the human element than the technology element to "assess and mitigate threats directly rather than rely on a script." SOC operatives continuously manage known and existing threats while working to identify emerging risks. They also meet the company and customer's needs and work within their risk tolerance level. While technology systems such as firewalls or IPS may prevent basic attacks, human analysis is required to put major incidents to rest.

For best results, the SOC must keep up with the latest threat intelligence and leverage this information to improve internal detection and defense mechanisms. As the InfoSec Institute points out, the SOC consumes data from within the organization and correlates it with information from a number of external sources that deliver insight into threats and

[32] Visit http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/, to download the latest version of the report. Site viewed 06 March 2017.

vulnerabilities. This external cyber intelligence includes news feeds, signature updates, incident reports, threat briefs, and vulnerability alerts that aid the SOC in keeping up with evolving cyber threats (already discussed in some detail above). SOC staff must constantly feed threat intelligence into SOC monitoring tools to keep up to date with threats, and the SOC must have processes in place to discriminate between real threats and non-threats.

Truly successful SOCs utilize security automation to become effective and efficient. By combining highly-skilled security analysts with security automation, organizations increase their analytics power to enhance security measures and better defend **against data breaches and cyber-**attacks. Many organizations that don’t have the in-house resources to accomplish this turn to managed security service providers that offer SOC services.[33]

7.2.4 The Emergency Communications Cybersecurity Center (EC3)

For a public safety specific cybersecurity solution, the FCC TFOPA WG1 reports recommended the creation of the Emergency Communications Cybersecurity Center (EC3). “In the TFOPA proposed architecture for NG9-1-1 Cybersecurity, the Emergency Communications Cybersecurity Center (EC3) will take on the role of providing Intrusion Detection and Preventions Systems (IDPS) services to Emergency Communications Centers (ECCs) and any other emergency communications service or system that would consider utilizing the centralized, core services architecture proposed. For example, not only ECCs but Emergency Operations Centers (EOCs) and virtually any State or Local public safety related communications services could also interconnect to the EC3.” [34]

This approach needs to be considered as part of the overall mitigation strategy for NG9-1-1. It has been well defined, researched, and cost estimates have even been developed based on existing technologies. In addition, while the name or who implements the solution is not important, the operational capabilities this approach and architecture brings is critical to success. More information on this solution is included in Appendix B of this report.

7.2.5 Managed Security Services Provider (MSSP)

According to Gartner, a managed security service provider (MSSP) provides outsourced monitoring and management of security devices and systems. Common services include managed firewall, intrusion detection, virtual private network, vulnerability scanning and anti-viral services. MSSPs use high-availability security operation centers (either from their own facilities or from other data center providers) to provide 24/7 services designed to reduce the number of operational security personnel an enterprise needs to hire, train and retain to maintain an acceptable security posture.[35] An MSSP is usually an Internet service provider (ISP) that provides an organization with some amount of network security management, which may include virus blocking, spam blocking, intrusion detection, firewalls, and virtual private network (VPN) management, as mentioned above. An MSSP can also handle system changes,

[33] This section is reproduced from https://digitalguardian.com/blog/what-security-operations-center-soc, viewed 06 March 2017.
[34] See http://www.gartner.com/it-glossary/mssp-managed-security-service-provider/, viewed 06 March 2017
[35] Based on text contained in TFOPA WG1 Supplemental Report, dated December 2, 2016, pp. 7-8.

modifications, and upgrades. MSSPs have evolved in various ways. Some traditional ISPs, noting the increasing demand for Internet security that has occurred in recent years, have added managed security to their repertoires. A few security vendors have added Internet access, thus becoming MSSPs. Still other MSSPs have come into existence as brand new entities.

An MSSP offers cost savings by allowing an organization to outsource its security functions. But some organizations are reluctant to give up complete control over the security of their systems. In addition, there may be considerable variability in competence among MSSPs.[36] The TFOPA-defined EC3 concept discussed above is a variant of the MSSP concept. Given the general lack of security expertise and capability at ECCs and in public safety organizations globally, looking at MSSPs to perform this function for ECCs and control rooms is strongly recommended, as the cost to hire and stand up internal security functions that can deal with the exploding number of security threats will be prohibitive for all but the largest and most well-funded centers.

7.2.6 Antivirus (AV) software

Antivirus software grew out of the reality that traditional computer operating system design paradigms were not able to stop “viruses” from “infecting” computer systems. Today’s virus checkers rely primarily on “signatures:” they match files against a database of code snippets of known viruses. The code matched can be part of the virus’ replication mechanism or its payload. The disadvantages of this sort of pattern-matching approach should be obvious. Unless you have some of the virus code signatures in the database, the AV software can’t scan for them, so if virus developers obfuscate or otherwise try to hide virus signatures, or AV databases are not kept up to date, viruses will be missed by the checker. A second approach, used somewhat today but likely to be a mainstay in the future, relies on anomaly detection. Anomaly detection relies on statistics; the properties of normal programs and documents are different than those of malware; the trick is to avoid false positives.

Antivirus software is not a fire-and-forget technology; it needs constant attention, both because of the changing threat environment and the changing computing environment. The need for up-to-date signature and anomaly databases should be quite clear. One of the most controversial issues surrounding AV software is on which machines it should be used. AV should be understood as one line of defense in a multi-layered defense system (which is discussed in more detail later in this paper). It protects against threats that an OS cannot catch, and it is also capable of blocking attacks that somehow managed to get through another protection layer. AV, more properly anti-malware, software is a mainstay of today’s security environment. Unfortunately, it is losing its efficacy.

So, should you run AV software in your environment? For generic desktop systems, the answer is probably yes. It’s relatively cheap protection and is usually trouble free. Similarly, server or firewall-resident scanners can block malicious inbound malware before it reaches users. All of this depends on keeping AV databases updated regularly.

[36] Taken from http://searchitchannel.techtarget.com/definition/MSSP, viewed 06 March 2017.

7.2.7 Firewalls and Intrusion Detection Systems

Since the dawn of the commercial Internet, firewalls have been a mainstay of security defense. That said, their utility, and in particular the protection they provide, has diminished markedly over the years. The original purpose of firewalls was to keep "bad guys" away from bugs inherent in internal computer code that could be exploited, but in a world awash in malware, phishing attempts, and the like, the original theory and use for a firewall is being challenged like never before. A firewall traditionally was a security policy enforcement device that takes advantage of a topological chokepoint. There are three properties necessary for a firewall to be effective:

1. A topological chokepoint must exist at which to place a firewall.
2. The nodes "inside" of the firewall share the same security policy
3. All nodes "on the inside" must be "good;" all nodes on the outside are, if not actually "bad," untrusted.

When one or more of these conditions cannot hold, a firewall cannot succeed. Today, none are true for the typical enterprise, including the (coming) IP-connected ECC, unless of course the network to which the ECC is connected is completely walled off from the Internet which would, unfortunately, defeat the entire promise and purpose of migrating to NG9-1-1 networks and systems! It is worth noting, however that with the exception of #3, none of these are absolute. Minor deviations in #1 or #2 are tolerable. But any deviation from these principles will limit the effectiveness of a firewall. It is also important to realize that no firewall can provide protection at any other layer of the protocol stack other than the one in which it operates. For example, a typical packet filter operates at layer 3 and a bit of layer 4 (the port numbers) and, as such, can filter by IP address and TCP port. It can't look at Media Access Control (MAC) addresses nor can it look inside e-mail messages. All of this has made today's firewalls more complex. Thus, regarding firewalls, some conclusions can be drawn:

- Small-scale firewalls, protecting a network about the size run by a single system administrator, still serve a useful function.
- Complex server applications are rarely amenable to firewall protection, unless the firewall has some very, very good (and very well written) sanitizing technology
- An enterprise firewall retains value against low-skill attackers but is actually a point of risk, not protection, when trying to filter complex protocols against sophisticated adversaries.
- Mobile devices, in general, should never be fully trusted, because of their likelihood of carrying malware.
- A traditional network architecture with a firewall that protects its "walled garden" assumes that network elements behind the firewall trust each other explicitly; these elements shouldn't.

An *intrusion detection system* (IDS) is a backup security mechanism. It assumes that your other defenses – firewalls, hardened hosts, etc. – have failed. The task then is to notice a successful attack as soon as possible, which permits minimization of the damage. Like AV software, IDS's can be signature or anomaly based; the same advantages and disadvantages apply. The key difference is in deployment scenarios; AV software operates on files and IDS's are generally classified as network or host intrusion detection systems. Host IDS's can operate on network or host behavior or content. Both the network and host IDS approaches has pluses and minuses. The big attraction of anything network based is scalability; like a firewall, a network IDS, many times installed on the same network element hosting the firewall, can watch over a network where many hosts are connected. The idea is to grab packets as they traverse the network ingress, scanning IP addresses and port numbers, looking for anomalies. Dealing with encrypted traffic is an issue and the possibility of missed packets also exists with network-based IDS. The fundamental problem with any form of network IDS is that it lacks context. It is difficult for even the best network scanners to re-assemble every packet in transit and then scan it for malware. This is much easier done on host IDS systems. Hosts can also look at log files, all but impossible to do at the network level, and can scan their own file systems for unexpected changes. Host-based IDS can also emulate network protocols, above the level of any encryption. There also specialized IDS systems that are aimed at so-called "extrusion detection," or trying to detect someone explicitly trying to steal your data and "extract" it out of your system.

An *intrusion prevention system* (IPS) can be described as an IDS that is also equipped to do some remediation if an anomalous security event is detected. An IPS can do many things; as with an IDS, it can be host or network resident; both have advantages and disadvantages. Depending on where it is located, it can block connections, quarantine files, modify packets, and more. The good functioning of an IPS rest on three foundations: very good detection, selection of countermeasures, and matching the countermeasures to confidence in identification of the root cause of the problem. For this reason, IDS and IPS systems are integrated into an IDS / IPS.

7.2.8 Cryptography and VPNs

The two most common uses of *cryptography* are to prove identity and to hide data from those who are not authorized to see it. It can do these things very well, but at a price, the most obvious being the encrypting keys have to be protected. When keys are exposed, the cryptography employed is rendered useless. A second major challenge to employing cryptography for information security is the difficulty in devising proper cryptographic mechanisms. Cryptography is a very difficult and subtle branch of applied mathematics; remarkably few people are qualified to practice it. NEVER use a proprietary encryption algorithm, especially if you are told that it's more secure because it is secret. The story of SSL 3.0 and the TLS protocol derived from it, are warning enough here.[37] A third issue with cryptographic-based security is that it is very difficult to retrofit cryptographic methods to existing systems, especially if there are complex communications systems or requirements. Ideally, cryptographic methods should be designed together with the system they are intended to protect. Unfortunately, "Greenfield" systems are rare. The two primary ways encryption is deployed in a system is *transport encryption*, where a real-time transport channel is being protected, and *object encryption*, where data must be protected across an arbitrary number of hops amongst arbitrary parties. You should

[37] Discussion taken from Bellovin, Steven M. *Thinking Security: Stopping Next Year's Hackers*. NY: Addison-Wesley, 2016, pp. 82 – 83. Though SSL was deprecated at the time the exploit was discovered, researchers discovered an exploit in SSL3.0 in 2014 that allowed decryption of intercepted traffic one byte at a time through making a large number of secure http requests downgrading from TLS to SSL to the originating server. See https://www.us-cert.gov/ncas/alerts/TA14-290A.

always use authentication with encryption; there are too many games an attacker can play if you don't. The most common layer of the protocol stack where transport encryption is done is at the application layer (Layer 7). In particular, TLS is heavily used for web transmission security and TLS is written into NG9-1-1 specifications. Object encryption is much harder than transport encryption because by definition you are not talking to another party when you encrypt something. Since a lost key has serious implications for object encryption, one should avoid using it unless the risk to the data you want to protect is VERY great.

Virtual Private Networks (VPNs) are intended to provide seamless, secure communications between a host and a network or two or more networks. The big advantage of VPNs is they provide "fire-and-forget" cryptography; once you turn one on, all of your traffic is protected. Although many VPN topologies exist, only two are common: connecting multiple locations of a single organization and connecting mobile devices back to the enterprise network. A VPN is intended to seem and operate like a real network, with one crucial difference; some of the "wires" of the network are in fact encrypted network connections that may pass through many other networks and routers. These links, or tunnels, are often treated like any other network links. Picking what VPN technology to use is harder than deciding that you need one. There are at least FIVE obvious choices: IPSec, Microsoft's Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), the Internet Engineering Task Force (IETF) version of PPTP that needs to run over IPSec to be secure, OpenVPN, and a larger group of so-called "TLS (or SSL) VPN" products of which there are TLS portal and tunnel VPNs. IPSec has the cleanest architectural vision. It is available on virtually all platforms, supports a wide range of authentication methods, and can secure more less anything layered on top of it.

Overall, protecting cryptographic keys is extremely important to using cryptographic security methods. Strong overall security will require different keys for different security levels, suitable software to let users manage such complexity, and a lot of user education and training on how to behave.

7.2.9 Identity Credentialing Access Management (ICAM)

ICAM encompasses standardized core capabilities to be able to identify, authenticate, and authorize individuals and provides appropriate access to resources, which is the lynchpin to the success of the national cybersecurity initiative. Detailed in this section are the high level ICAM goals and objectives, and a reference to the Federal Government's implementation of Identity, Credential, and Access Management (FICAM).

The FICAM information detailed in the following section is derived, or directly sourced, from Federal ICAM documents[38] and NIST Special Publication 800-63-2. The information referenced below provides public safety officials with insight into federal initiatives aimed at securing government systems through the establishment of credentialing and management techniques. The information provides potential modeling for local authorities and is intended only as a reference and education source.

[38] https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/FICAM_Roadmap_and_Implem_Guid.pdf

The intent of the ICAM discussion in this report is not to suggest that local, regional, or State agencies be required to utilize any type of Federal single user, single sign-on approach. Rather, the intent is to provide an education as to the need for identity control and access management at all levels of interface.

When properly aligned, ICAM creates a basis for trust in securely enabling electronic transactions, which should include secure access to facilities and installations. Just as identity, credential, and access management activities are not always self-contained and must be treated as a cross-disciplinary effort, ICAM also intersects with many other IT, security, and information sharing endeavors. Some of the most relevant of these include privacy impacts of the ICAM segment architecture, implementation considerations for network and device authentication, and ICAM as a component of information sharing. However, many of these overlapping and dependent disciplines are too broad and far-reaching to be covered in this document. It is expected that ICAM will touch many initiatives not specifically and will be incorporated into holistic agency plans for their Enterprise IT, Mission and Business Service Architectural Segments.

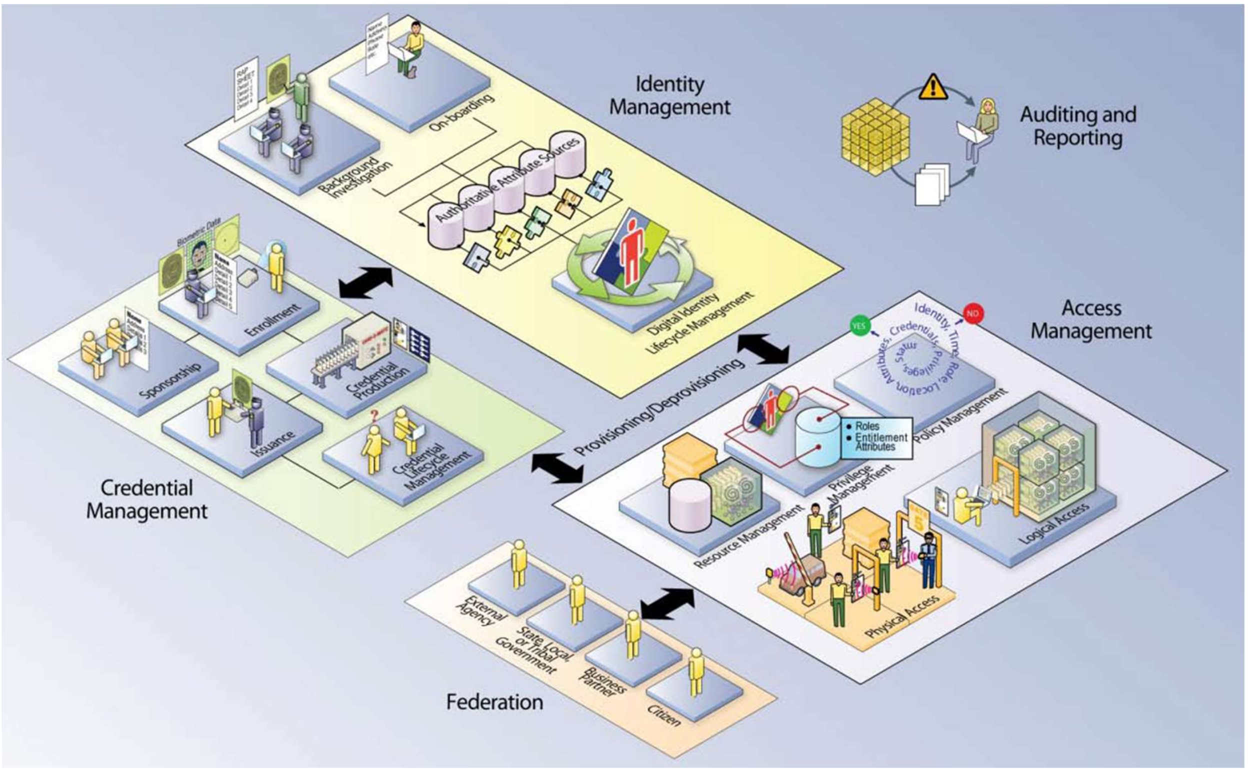


Figure 7-1: - ICAM - The Big Picture

7.2.9.1 PKI: Public Key Infrastructures

PKI, or public key cryptography, originally described in 1976, is a security method using encryption keys to send secure messages. Someone uses your available and published public key to encrypt a message to you, and you, in turn, use your private key to decrypt it. The trick to making PKI-based security work is how cipher keys are distributed and how the systems that provide them are themselves administered and secured. In 1978, the method of using "certificates," a digitally signed message containing a user's name and public enciphering key, was devised to exchange public keys. Today, certificates are embedded in a framework known as Public Key Infrastructure, or PKI. The Internet Security Glossary defines PKI as "The set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates based on asymmetric cryptography." Proper functioning PKI is about more than just code; it is a SYSTEM. Most PKI certificates use the X.509 standard and are very complex in nature. The fundamental questions about certificates are about security: who signs the certificates? Do you trust them? Are they honest? Are they competent, both at procedures and technically? These questions, and their answers, lie at the heart of a well-functioning security system based on PKI.

When you use a certificate in this way, you are relying on the trustworthiness of the issuer. The heart of the certificate system is the certificate authority, or CA. A CA does just what the name implies, i.e., issues certificates. The crucial limitations of certificate-based systems include:

- It is rarely clear to system administrators or developers which CAs are trusted for given applications. It is almost never clear to end users.
- It is rarely clear to anyone what a given certificate's intended use is.
- It is almost never clear how trustworthy or competent a CA is.

All of this indicates that standard Internet-wide PKI as it exists today is unacceptably insecure; however, most of the tools and pieces of a PKI-based infrastructure can be used quite securely if the three problems identified above are addressed. That is, if a scenario can be devised in which everyone knows exactly WHO can issue a certificate and what the purpose of that certificate is and if the issuers can be trusted to an extent commensurate with the resource being protected, you can have a secure (or secure enough) system while using the same software, syntax, etc. of existing X.509 certificate-based systems. This avoids the major issue with web-based PKI systems that exists today, namely the "let a hundred CAs bloom" approach of browser and OS vendors. Trustworthiness is the key issue in PKI.

A more detailed discussion of PKI can be found in Appendix A of this document.

7.2.9.2 Authentication Methods

Authentication is generally considered to be one of the most basic security principles. Absent bugs, authentication effectively controls what system objects someone can use. In other words, it is important to get authentication right. There are three (3) basic forms of information that can serve as the basis of an authentication system: something you know (e.g., a password), something you have, such as a token or a particular mobile phone, or something you are, that is some form of biometric.

The classic authentication method, passwords, has generated and continues to generate discussion regarding how best to employ them and how actually effective they are. The need for strong, un-guessable passwords, clashes with usability of systems in the real world, and realistic systems try to balance both imperatives. As the threat model has changed, ideas about what constitutes the "best passwords" has changed with it. What type of password discipline to enforce depends on the answers to certain questions about your system design:

1. What types of guessing attacks are you trying to guard against, online (where the attacker actually tries to login) or offline, based on a stolen hashed password file?
2. Are the passwords in question employee passwords or user passwords?
3. More generally, are you concerned with opportunistic or targeted attacks?
4. What do you assume the enemy can do? Subvert client machines? Subvert your servers? Launch phishing attacks? Bribe employees? Eavesdrop on conversations?

Some commentators think biometric authentication systems might be a solution to the password conundrum, but consider this: a biometric authentication system consists of a number of components: a human, a sensor, a transmission mechanism, a biometric template database, and an algorithm at a minimum. An attack can target any one of these, which means that they must all be protected. Biometric authentication also involves the thorny issue of privacy. A biometric identifier is more or less the ultimate form of PII. Using biometric authentication unnecessarily not only puts you at risk to violate privacy laws, it also exposes organizations to serious public relationship problems should the signature database be stolen. The decision to use biometric authentication should not be taken lightly.

Tokens, something you have, are a popular authentication mechanism for security-sensitive organizations. Using tokens avoids all of the weaknesses of passwords, but they can be more expensive (tokens cost money), and it may be unknown whether all relevant applications in an environment can be adapted to use tokens. Perhaps the biggest incompatibility is the mismatch between applications that instantiate many sessions over time and the single-use property of most token-based systems.

While no one authentication system is suited for meeting all requirements, all of the time, some conclusions, or observations, about passwords can be drawn from this brief consideration of authentication technologies:

- Passwords are not suitable, ideally, for high-security needs. Making plans to move away, or beyond, passwords makes sense in these environments if the threat model indicates passwords will be a weakness.
- That said, passwords are not going away anytime soon, since converting applications to stronger authentication methods will be, if nothing else, time consuming. In the interim, as the switch is made to stronger authentication methods, use of password managers (do your homework on which one is best for your needs) will help with password reuse and strength problems.
- Implement bilateral authentication (its strong protection against phishing). Some password managers do this automatically; they will send a password only they recognize to the site and they are not fooled by clever e-mail messages
- Master passwords are especially crucial and need the best protection. These, for sure,

need to be as strong as possible.

- Plan for exceptions; know in advance how you will handle lost or stolen passwords, compromised servers, and the like.

It is important to note that there are fads in authentication that go in and out of style over the years. Each organization should decide on the best authentication technology that matches its particular threat mode and operational environment. Perhaps the "one to watch" in the next few years is the single sign on, or "federated" approach to authentication. Both the TFOPA WG1 Final and Supplemental Reports, referred to earlier in this document, have a good discussion regarding efforts at the US Federal level to address the need for better authentication methods in public safety and well worth reviewing from this standpoint.[39]

7.3 Information Spoofing Mitigation

Use Cases #2 and 3, described in Sections 7.1.2 and 7.1.3 , respectively, discuss the use of caller identity spoofing in the context of TDOS and SWATTING attacks. Illegitimate caller identity spoofing is a growing concern for North American telephone service providers and their customers. With the introduction of IP-based telephony, caller identity spoofing is easier and more affordable than ever before. To combat illegal spoofing, the industry has developed standards for the authentication and verification of caller identity information for calls carried over an IP network using the Session Initiation Protocol (SIP). The Signature-based Handling of Asserted Information Using toKENs (SHAKEN) standards developed by the Alliance for Telecommunications Industry Solutions (ATIS), as well as specifications developed by the Internet Engineering Task Force (IETF) Secure Telephone Identity Revisited (STIR) Working Group, allow calls traveling through interconnected carrier networks to have the legitimacy of their caller identity evaluated and, if asserted, "signed" as legitimate by the originating carrier. The terminating carrier performs validation checks against the signed caller identity before the calls are delivered to called users, allowing the carrier of the party receiving the call to provide an indication to the called party of the legitimacy of the caller identity information.

In an end-state NG9-1-1 environment, SHAKEN authentication and verification services and associated protocols can be used to mitigate caller identity spoofing in the context of 9-1-1 calls as well as to emergency callbacks. For 9-1-1 calls, interactions between originating network elements and the SHAKEN authentication service can be used to support caller identity assertion and signing. Interactions between elements of the NG9-1-1 Emergency Services Network and the SHAKEN verification service, will allow the signed caller identity information to be verified. The attestation level and verification status information, indicating the trustworthiness of the caller identification (e.g., the emergency caller's callback number) information, can then be delivered to the ECC along with the callback number. Interactions with the SHAKEN architecture and procedures to support caller authentication can also be used in the context of emergency callbacks that are routed via an NG9-1-1 Emergency Services Network, with authentication provide by the NG9-1-1 Emergency Services Network, and verification provided by the emergency caller's home network. Application of SHAKEN procedures to emergency

[39] See TFOPA WG1: Optimal Cybersecurity Approach for PSAPs, Final Report, 10 December 2015, pp. 9-12 and 19 -23 and Supplemental Report, 2 December 2016, pp. 22-27.

callbacks in an end-state NG9-1-1 environment may increase the chance of the call completing to the called party, which is an important feature for emergency callbacks. The ability to recognize spoofed caller identities may provide Public Safety a critical tool to support the detection and mitigation of Telephony Denial Of Service (TDOS) and SWATTING attacks.

In addition to the caller identity authentication/verification provided by the SHAKEN framework, other information associated with 9-1-1 calls and emergency callbacks in and end-state NG9-1-1 environment may also be spoofed. For this reason, the industry is defining procedures to use the SHAKEN framework to support the signing and verification of the SIP Resource-Priority Header (RPH) and Priority header fields. The SIP RPH field may be used by SIP user agents, including Public Switched Telephone Network (PSTN) gateways and terminals and SIP proxy servers, to influence the prioritization of resources afforded to certain types of communication sessions. Since the SIP signaling associated with 9-1-1 originations and emergency callbacks includes an RPH, there is concern that the SIP RPH field could be spoofed and abused by bad actors, impacting the processing of 9-1-1 and emergency callbacks.

In and end-state NG9-1-1 environment, if an ECC determines that it is necessary to call an emergency caller back (e.g., if the caller disconnects prematurely) it can use a SIP Priority header to mark such calls (i.e., using a value of “psap-callback”). This marking will allow special network handling of the call, such as bypassing services that might preclude the call from completing. Since the SIP Priority header field may affect routing and call handling, there is value in applying the concepts of authentication/signing and verification to this information as well caller identity and RPH information.

The SWATTING use case described in Section 7.1.3 also suggests the need to mitigate spoofing of location information in an end-state NG9-1-1 environment. Public Safety would benefit from industry support for a mechanism, comparable to the signing/verification mechanism that has been specified for caller identity information, that would provide an indication of the trustworthiness of the location information associated with a 9-1-1 call. Considerations related to potential solutions that would allow for the “signing” and “verification’ of location information need to address the fact the location may be delivered “by value” or “by reference”. In addition, mechanisms for mitigating location spoofing should take into account the source of the location information (e.g., whether the location was generated by location technology within the carrier network or was received from the device) and whether any kind of “sanity checks” have been performed on the information as part of the authentication process. The concept of signing location information requires further study.

Because the SHAKEN framework relies on the transmission of information via SIP messaging, it can only operate on the IP portions of a service provider’s network. During the transitional state and in the legacy state of 9-1-1, some if not all of the main components of the service architecture will not be SIP-enabled, making SHAKEN, as currently defined, not feasible as a spoofing mitigation mechanism.

In a transitional environment, where an NG9-1-1 Emergency Services Network is in place, but the originating network is a legacy network, additional mechanisms would need to be defined to allow the originating network to attest to and sign caller identity information. It is also possible that a gateway system on the ingress side of the NG9-1-1 Emergency Services Network could interact with an authentication service and pass signed caller identity and other information to the NG9-1-1 Emergency Services Network, but without some input from the originating network provider related to the trustworthiness of the caller identity, the gateway would need to associate the lowest level of attestation with the caller identity. The NG9-1-1 Emergency Services Network could perform SHAKEN validation on the caller identity if it had a way of obtaining the SHAKEN authentication information. Since a gateway on the ingress side of the NG9-1-1 Emergency Services Network would be populating the RPH, it could also interact with an Authentication Service to sign that information, and the NG9-1-1 Emergency Services Network could verify the signed RPH.

In a transitional 9-1-1 environment where the 9-1-1 call is delivered to a legacy PSAP via a gateway on the egress side of the NG9-1-1 Emergency Services Network, existing legacy interfaces would not support the conveyance of the results of the caller identity authentication and verification process to the PSAP call taker. Further study is needed to determine the feasibility of making any changes to the legacy interfaces to support the delivery of caller identity authentication/verification information to legacy PSAPs in a transitional 9-1-1 environment.

In a legacy 9-1-1 environment, where there is no SIP capability in the originating network, Emergency Services Network, or the PSAP, the SHAKEN spoofing mitigation mechanism will not apply. While there is currently industry activity focused on identifying and analyzing call authentication mechanisms for use in a non-IP environment, there are some unique characteristics of legacy 9-1-1 architectures that may present additional challenges. For example, while many legacy 9-1-1 implementations use SS7-based dedicated trunk groups to interconnect wireline end offices or MSCs with SRs, there are still legacy 9-1-1 implementations that use dedicated MF trunks between legacy originating networks and SRs for 9-1-1 call delivery. Unlike the routing of non-emergency calls, call routing of 9-1-1 calls relies on mappings of calling party number/ANI/pANI information to PSAP routing information. Call delivery from the SR to the PSAP also uses MF trunks. Any caller identity authentication mechanism used in a legacy 9-1-1 environment must not significantly increase the call setup time associated with 9-1-1 calls.

7.4 Detect Function

7.4.1 Information Sharing Environments

The importance of information sharing cannot be understated. In the current environment, ECCs perform multiple critical functions for their jurisdiction. Many of these functions are common across all lines of operation and regardless of locality. However, the ability to share information in real time, between multiple ECCs, agencies, and jurisdictions has not been refined. As part of the overall approach to cybersecurity, it is crucial that ECCs, 9-1-1 Authorities, and the agencies they all support, are able to share intelligence in a real time, or near real time environment.

While we have not yet made the transition to all IP networks and systems, the opportunity exists today to participate in a number of information sharing environments (ISEs) which are designed to share data, best practices, and resources amongst multiple elements within the public safety community. To date, many of these remain underutilized.

7.4.2 DHS Cybersecurity and Infrastructure Security Agency (CISA)

DHS offers a collection of programs and initiatives that can be applied to reduce NG9-1-1 cyber risks. Many of these efforts support approved missions that cover Federal, State and local users, as well as public and private critical infrastructure entities.
See https://www.cisa.gov/cybersecurity.

Federal, State and Local Partnerships and Forums. DHS has formed existing relationships across all levels of government to inform the design and deployment of emergency communication networks. DHS supports SAFECOM and the National Council of Statewide Interoperable Coordinators bringing State, local, Tribal, and Territorial perspective to a National forum. DHS has partnered with the U.S. Department of Transportation (DOT) NG9-1-1 Program Office to facilitate education and awareness of cybersecurity with the State and local community through the delivery of tools and training. DHS also facilitates the Emergency Communications Preparedness Center (ECPC) 9-1-1 Focus Group, which is dedicated to enhancing the resiliency of Federal PSAP (or ECC) operations.[40] Additionally, DHS manages the Emergency Services Sector (ESS) Cyber Working Group to evaluate cyber risks that the sector might encounter.[41]

Assessments and Analysis: DHS, in conjunction with the DOT National 9-1-1 program, is currently developing an NG9-1-1 security best practice and self-assessment tool for PSAPs (or ECCs), Cyber Risks to Next Generation 9-1-1.[42] Additionally, DHS is working on next steps on the development of Identity, Credential, and Access Management (ICAM) for public safety and FirstNet's National Public Safety Broadband Network. The through the ESS Cyber Working Group mentioned above, the Department has published the DHS Internet Protocol (IP) Emergency Services Sector Cyber Risk Assessment[43] and Emergency Services Sector Roadmap to Secure Voice and Data Systems[44] which provide pertinent guidance for public safety agencies, including those considering the adoption of NG9-1-1 technology and systems to strengthen their systems and networks against cyber risk through mitigation measures.

Public / Private Collaboration: The Critical Infrastructure Cyber Information Sharing and Collaboration Program (CISCP) establishes trusted cyber information sharing relationships across Government and Industry. CISCP facilitates the secure exchange of cybersecurity indicators, enabling organizations to protect themselves against emerging attacks. Currently, CISCP has over one-hundred member organizations and is working in collaboration with the

[40] Office of Emergency Communications, http://www.dhs.gov/office-emergency-communications.
[41] https://www.dhs.gov/xlibrary/assets/nipp-ssp-emergency-services.pdf
[42] Cyber Risks to Next Generation 9-1-1, available at http://www.dhs.gov/office-emergency-communications.
[43] DHS Internet Protocol (IP) Emergency Services Sector Cyber Risk Assessment.
https://www.dhs.gov/sites/default/files/publications/Emergency-Services-Sector-Cyber-Risk-Assessment-508.pdf
[44] ESS Roadmap to Secure Voice and Data Systems.
https://www.dhs.gov/sites/default/files/publications/Emergency-Services-Sector-Roadmap-to-Secure-Voice-and-Data%20Systems-508.pdf

NCCIC to automate cybersecurity information sharing amongst its members.[45]

User Training and Education: DHS provides resources for cybersecurity training and awareness, for use by any public or private entity. These resources can be leveraged to provide users with a basic level of awareness of cybersecurity risks. In many instances, cyber threat actors exploit untrained individuals (*e.g.,* phishing attacks) to gain initial access to the enterprise and initiate further actions. The "Stop. Think .Connect. Campaign" is geared to provide awareness.[46] DHS also supports the National Initiative for Cybersecurity Education (NICE), which provides additional educational resources for public and private organizations.[47] DHS also delivers education and technical assistance to Federal, State and local public safety community on ECC deployments.

Outreach and Assistance: The Critical Infrastructure Cyber Community C^3 (pronounced "C Cubed") Voluntary Program (C^3VP) supports organizations of all sizes to establish or improve their cyber risk management processes and to take advantage of free technical assistance, tools, and other resources offered by the U.S. Government. C^3VP can assist ECCs in understanding how to use NIST's Cybersecurity Framework and other risk management efforts.

7.4.3 US-CERT

United States Computer Emergency Readiness Team (US-CERT) brings advanced network and digital media analysis expertise to bear on malicious activity targeting our nation's networks. US-CERT develops timely and actionable information for distribution to federal departments and agencies, state and local governments, private sector organizations, and international partners. In addition, US-CERT operates the National Cybersecurity Protection System (NCPS), which provides intrusion detection and prevention capabilities to covered federal departments and agencies.

US-CERT strives for a safer, stronger Internet for all Americans by responding to major incidents, analyzing threats, and exchanging critical cybersecurity information with trusted partners around the world.

US-CERT's critical mission activities include:

- Providing cybersecurity protection to Federal civilian executive branch agencies through intrusion detection and prevention capabilities.
- Developing timely and actionable information for distribution to federal departments and agencies; state, local, tribal and territorial (SLTT) governments; critical infrastructure owners and operators; private industry; and international organizations.
- Responding to incidents and analyzing data about emerging cyber threats.
- Collaborating with foreign governments and international entities to enhance the nation's cybersecurity posture.

[45] (https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity)
[46] (http://www.dhs.gov/stopthinkconnect)
[47] (http://csrc.nist.gov/nice/index.htm)

7.5 Respond Function

7.5.1 Security Incident and Event Management (SIEM) Systems

According to Gartner: Security information and event management (SIEM) technology supports threat detection and security incident response through the real-time collection and historical analysis of security events from a wide variety of event and contextual data sources. It also supports compliance reporting and incident investigation through analysis of historical data from these sources. The core capabilities of SIEM technology are a broad scope of event collection and the ability to correlate and analyze events across disparate sources.[48] Security information and event management (SIEM) is an approach to security management that seeks to provide a holistic view of an organization's information technology (IT) security. The acronym is pronounced "sim" with a silent e. The underlying principle of a SIEM system is that relevant data about an enterprise's security is produced in multiple locations and being able to look at all the data from a single point of view makes it easier to spot trends and see patterns that are out of the ordinary. SIEM combines SIM (security information management) and SEM (security event management) functions into one security management system.

A SEM system centralizes the storage and interpretation of logs and allows near real-time analysis which enables security personnel to take defensive actions more quickly. A SIM system collects data into a central repository for trend analysis and provides automated reporting for compliance and centralized reporting. By bringing these two functions together, SIEM systems provide quicker identification, analysis and recovery of security events. They also allow compliance managers to confirm they are fulfilling an organization's legal compliance requirements.

A SIEM system collects logs and other security-related documentation for analysis. Most SIEM systems work by deploying multiple collection agents in a hierarchical manner to gather security-related events from end-user devices, servers, network equipment -- and even specialized security equipment like firewalls, antivirus or intrusion prevention systems. The collectors forward events to a centralized management console, which performs inspections and flags anomalies. To allow the system to identify anomalous events, it's important that the SIEM administrator first creates a profile of the system under normal event conditions. At the most basic level, a SIEM system can be rules-based or employ a statistical correlation engine to establish relationships between event log entries. In some systems, pre-processing may happen at edge collectors, with only certain events being passed through to a centralized management node. In this way, the volume of information being communicated and stored can be reduced. The danger of this approach, however, is that relevant events may be filtered out too soon.

SIEM systems are typically expensive to deploy and complex to operate and manage. While Payment Card Industry Data Security Standard (PCI DSS) compliance has traditionally driven SIEM adoption in large commercial enterprises, concerns over advanced persistent threats

[48] See http://www.gartner.com/it-glossary/security-information-and-event-management-siem/, viewed 06 March 2017.

(APTs) have led smaller organizations to look at the benefits a SIEM managed security service provider (MSSP) can offer.[49]

7.6 Recover Function

Once an ECC is affected by a Cyber Incident, the Recovery Function is used to restore proper operational capabilities. Certain precautions should be taken in order to facilitate the Recovery process and to reduce time and costs of the effort. Two key areas of preparation are recommended.

A variety of recovery functions are outlined in the use cases above as well as in any set of industry recognized cybersecurity controls such as those described in this Report.

7.6.1 Cyber Insurance

As stated throughout this document, it is a matter of when, not if, any network will experience some sort of compromise. Accordingly, it is not surprising that there is a growing cybersecurity insurance industry; PWC (PwC refers to the global accounting and advisory firm formerly known as PricewaterhouseCoopers) estimated in 2018 that the cybersecurity insurance market could be as large as $5.5 billion by 2021. [50] So, the thinking goes: if it is certain that at an uncertain time the network will experience a compromise, then it is a good idea to buy insurance. While CSRIC declines to recommend specifically whether or not organizations invest in cybersecurity insurance, it does note a growing market and the reasoning behind buying such insurance.

The purpose of cybersecurity insurance is clear: compromises have financial impacts, whether that is in lost productivity, exposure of or destruction to confidential information, civil liability, interruption to business, fines or other legal exposure, bad PR, or in the case of ransomware, a direct cash outlay. Insurance is designed to mitigate the financial impact to these compromises, which can come at any time. And so, cybersecurity insurance insures against the financial impacts of cybersecurity events.

An organization may feel that it has less of an obligation to implement a rigorous cybersecurity regime if it determines it is less expensive to insure against problems and simply buy their way out of them. This is absolutely not a recommended approach; an organization cannot look to insurance as a baseline security mechanism. Indeed, it covers only one of five threat detection domains described in this report; insurance does not identify, protect, detect or respond to a security vulnerability. At best, it constitutes only part of the fifth domain, that of recovering, without dealing with any of the vulnerabilities that led to buying insurance in the first place. Any organization that considers investing in insurance should do so without reducing any focus on

[49] This section taken from http://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM , viewed 06 March 2017.
[50] See *Are insurers adequately balancing risk & opportunity? Findings from PwC's global cyber insurance survey*, retrieved 4 May 2020 at https://www.pwc.com/us/en/industry/assets/pwc-cyber-insurance-survey.pdf.

other aspects of cybersecurity. It is to be considered only as a supplemental element of any security strategy.

7.6.1.1 Insurance and Ransomware

Media reports and research in the cybersecurity industry recount a troubling blossoming of ransomware attacks; security firm Emsisoft reports that thousands of ransomware attacks occurred in 2019, including at least 966 government agencies, some of which affected 9-1-1 operations. [51] In the context of insurance for cyber-attacks, ransomware is a very clear-cut application—ransomware operators want a cash payout, and an insurance policy provides the insured with ready access to cash with minimal direct financial penalty outside of a deductible and a potential impact to premiums. For example, the National Association of Insurance Commissioners reports that one jurisdiction in Florida paid just a $10,000 deductible on a ransomware payout of nearly a half million dollars. [52] The same report explains that year-over-year ransomware detections overall in the United States rose by 365% from 2018-2019. [53]

Best practice dictates that, rather than rely on insurance, a good cybersecurity program is one that does not result in a successful ransomware attack in the first place, and comes, in part, from a combination of the methods described in this report. Buying one's way out of a ransomware attack does not recover the lost time, productivity or business operation that elapsed during the period that systems were locked down. Even worse, approaching ransomware with a default strategy of "buy insurance" provides greater incentives for ransomware operators in the first place; if they know that an organization has insurance and won't hesitate to use it, they know that they have a victim who may be ready and willing to pay. Each time an organization pays a ransom, they reinforce to criminal industry that ransomware is a lucrative and dependable business model.

7.6.1.2 Cyber Insurance in a Public Safety Context

Public safety and 9-1-1 introduce a dynamic unique only to a few industries: the health and life safety of the public. If, for example, an ECC is hit with a ransomware attack and unable to answer 9-1-1 calls or operate their dispatch consoles, [54] it does not matter that the organization has an insurance policy and can pay the ransom. It takes time to negotiate the terms of the ransom, to get clearance to invoke the insurance policy and pay the requisite deductible, to get an agreement from the insurer to pay damages, and to deposit the required cryptocurrency in the extorter's wallet. This is just the beginning, since full recovery and restoration of all systems is still required. It must be remembered that a cyber-criminal has invaded the ECC, possibly leaving behind modified data, additional malware or backdoors that would allow the criminal to regain access to the ECC. Paying the ransom does not do much to reduce the time and effort required to Recover from this type of Cyber Incident. During this time, public safety is

[51] See *The State of Ransomware in the US: Report and Statistics 2019*, retrieved 4 May 2020 at https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/.

[52] See *Ransomware*, updated 16 December 2019, Center for Insurance Policy and Research, National Association of Insurance Commissioners, retrieved 4 May 2020 at https://content.naic.org/cipr_topics/topic_ransomware.htm.

[53] See *Id.*

[54] A widely-publicized ransomware attack incapacitated Baltimore's 9-1-1 calltaking and dispatch systems for 17 hours in 2018. See public reporting, e.g., NBC News coverage at https://www.nbcnews.com/news/us-news/baltimore-s-911-emergency-system-hit-cyberattack-n860876, retrieved 4 May 2020.

jeopardized.

It is difficult enough to try to quantify the value of a life; it would be inexcusable for a public official to justify bad public safety outcomes directly caused by lax security on the basis that they had a sound Cyber Insurance plan. Many enterprises can measure the cost of their decisions based on financial risk and reward. The operation of life-saving 9-1-1 emergency calling systems does not provide that option. Public safety cannot evaluate topics like ransomware from a purely financial perspective. In that vein, while cybersecurity insurance can provide some help with the financial impacts of exploits, it does nothing to address the core mission of protecting the safety of life and property.

7.6.1.3 Should the ECC pay the Ransom?

Cyber experts have differing views on whether an agency impacted by ransomware should pay the ransom. The FBI recommends AGAINST paying the ransom[55]. But operational considerations for ECCs are unique because of the potential for loss of life and property. In general, the decision to pay the ransom should be focused on the loss of critical operational information to the ECC. First, attempts should be made to rely on backup ECCs or cross-jurisdictional support agreements to restore the 9-1-1 functions to citizens supported by the ECC. Next, attempts should be made to restore the lost data from data backups. If data backups fail to restore critical information impacted by the ransomware attack, the ECC should evaluate the cost (both in money and time) of recreating the lost information. If recreating the data is not possible, or comes at a cost that is significantly higher than the cost of paying the ransom, or requires an exorbitant amount of time, serious consideration should be given to paying the ransom in order to restore the lost critical data.

7.6.1.4 Problems with paying the ransom

First and foremost, it must be remembered that paying the ransom will reward criminal behavior. FBI Cyber Section Chief Herbert Stapleton warns that paying the ransom “really just encourages and facilitates further criminal activity. They [the hackers] basically will continue to attack as long as it’s profitable for them. So, continuing to contribute to that profitability just encourages more ransomware attempts.” [56]

Some of the cyber-criminals who use ransomware as their attack methods have been known to support terrorist organizations. David S. Cohen Undersecretary of the Council on Foreign Relations has indicated that payments to criminals using Ransomware to hold data hostage may run afoul of banking laws and policies as well as related statutes and regulations. Individuals and organizations choosing to make ransom payments to end Ransomware attacks could be subject to international sanctions programs administered in the U.S. by the Office of Foreign Assets Control (“OFAC”) and that ransom payments to Foreign Terrorist Organizations (“FTOs”) or Specially Designated Global Terrorists (“SDGTs”) identified by OFAC are illegal under U.S. law. [57] In particular, one very damaging ransomware strain, “SamSam”, was traced by the

[55] https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware

[56] https://www.fbi.gov/audio-repository/ftw-podcast-ransomware-082219.mp3/view

[57] David S. Cohen, *Kidnapping for Ransom: The Growing Terrorist Financing Challenge*, Council on Foreign Relations, Oct. 5, 2012.

Department of Justice to two cybercriminals[58] with ties to Iran and the paying of ransoms associated with SamSam were noted as possibly supporting terrorist activities. [59]

Paying the ransom is no guarantee that the victim will receive proper decryption tools and recover the lost data. A survey conducted by CyberEdge Group in 2018 discovered that of the 38.7% of the ransomware victims who paid the ransom, less than half (19.1%) recovered their files using the tools provided by the ransomware authors. [60]

7.6.1.5 Cyber Insurance helps but is no panacea

Insurance only should be considered as part of the overall approach to cybersecurity, not as a standalone solution or proactive 'fix' to the underlying issues. Fundamentally, insurance does not address any underlying problems, and short of reimbursing an organization for a paid ransom or costs to Recover services, it does not actually fix any immediate problems. An insurance policy does nothing to address the root cause: a vulnerability that was not sufficiently protected. This is especially important in a 9-1-1 context, where an exploit of the 9-1-1 system can result in the loss of human life during an emergency. Accordingly, while CSRIC VII acknowledges the growth of the cybersecurity insurance market, it cautions that insurance is *not* to be considered as a replacement for any of the other methods described in this report. Indeed, CSRIC VII advises that any organization with cybersecurity insurance should run its business as if it did not have any.

[58] https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-samsam-ransomware-press
[59] https://www.cfr.org/backgrounder/state-sponsors-iran
[60] https://www.bleepingcomputer.com/news/security/only-half-of-those-who-paid-a-ransomware-were-able-to-recover-their-data/

7.7 Considerations Related to the Use of Controls During the Transition

Controls can be used to provide actionable, material improvements in the cybersecurity posture of 9-1-1 in the United States. The Center for Internet Security® (CIS)[61] provides a widely industry-recognized model for improving cybersecurity practices at organizations ranging from small to large in its 20 CIS Controls.[62] IT security personnel use CIS Controls to establish the cybersecurity protection in their organizations. The controls defined by CIS are prioritized and prescriptive and provide a clear roadmap for organizations to gradually improve their cybersecurity posture, the use of which can help eliminate the most common attacks organizations experience. These controls align with the NIST cybersecurity framework and provide a practical approach for implementing practices that adhere to NIST guidelines; that is, to identify, protect, detect, respond to, and recover from cybersecurity threats. The following analysis examines how the 20 CIS controls can be adapted and applied to legacy, transitional and end-state NG9-1-1 environments. This analysis is based on an adaptation of Version 7.1 of the CIS controls,[63] which address NIST 800-53, Recommended Security Controls for Federal Information Systems and Organizations. A full mapping is available from CIS.[64] These controls describe a set of cybersecurity actions that can be used to address the Use Cases described above, with special circumstances around the maturity states, addressed in Section 3.3, *Methodology*. These controls can be adapted and deployed by organizations across the public safety ecosystem, especially those involved in 9-1-1.

7.7.1 The Controls

CIS recommends that every organization should strive to implement all 20 controls through the Implementation Group methodology. This framework could be applied at every level of the 9-1-1 ecosystem. Some of the controls expect a level of cybersecurity maturity that may not exist in all public safety agencies. Such maturity includes resources, staffing, funding, and policy implementation; and it may take time to implement all of the controls identified. Organizations going through the NG9-1-1 transition should consider adopting as many of these controls as possible. It is important to understand that the markings in the Table in Appendix D - Applying CIS Controls for the NG9-1-1 Transition, identify which controls one would EXPECT organizations to implement during each phase. If possible, organizations should strive to implement the full set of controls wherever practicable, but as organizations mature, the tables indicate EXPECTED control implementation beyond the merely aspirational.
The table below shows each of the 20 controls.

[61] CIS is a chartered nonprofit with an independent board and a recognized leader in internet security. Through the Multistate Information Sharing and Analysis Center (MS-ISAC), a partnership with US DHS, US-CERT and others, CIS provides free security resources to state, local, territorial and tribal governments and non-profit institutions.

[62] See CIS Controls, Version 7.1, Center for Internet Security, April 1, 2019. Retrieved August 7 2020 at https://www.cisecurity.org/controls/.

[63] CIS Controls are incorporated in part under CIS' Creative Commons Attribution-Non Commercial-No Derivatives 4.0 International Public License. See Id. At 2.

[64] See CIS Controls V7.1 Mapping to NIST CSF. Retrieved 11 August 2020 at https://www.cisecurity.org/white-papers/cis-controls-v7-1-mapping-to-nist-csf/.

Table 3: The 20 Controls

#	Control
1	Inventory and Control of Hardware Assets
2	Inventory and Control of Software Assets
3	Continuous Vulnerability Management
4	Controlled Use of Administrative Privileges
5	Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6	Maintenance, Monitoring and Analysis of Audit Logs
7	Email and Web Browser Protections
8	Malware Defenses
9	Limitation and Control of Network Ports, Protocols, and Services
10	Data Recovery Capabilities
11	Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12	Boundary Defense
13	Data Protection
14	Controlled Access Based on the Need to Know
15	Wireless Access Control
16	Account Monitoring and Control
17	Implement [an Institutional][65] Security Awareness and Training Program
18	Application Software Security
19	Incident Response and Management
20	Penetration Tests and Red Team Exercises

Each control includes up a 10-20 sub-controls; for example, Control 4, Controlled Use of Administrative Privileges includes 9 sub-controls, ranging from basic, easy-to-implement procedures like changing of default passwords to more sophisticated measures like requiring multi-factor authentication or use of dedicated workstations for all administrative access. Each sub-control, is in turn, mapped to a security function (Identify, Protect, Detect and Respond) as defined in the NIST CSF as well as an asset type (User, Device, Network and Data). Proposed mappings of all CIS controls to a legacy, transitional, and end-state NG9-1-1 environment as well as whether they apply to the PSAP/ECC, regional authority or state equivalent ESInet are included in Appendix D - Applying CIS Controls for the NG9-1-1 Transition. In general, familiarity with these mappings is a prerequisite for understanding this analysis.

An example of Control 4 and its subgroups is in the table below.

Table 4: Control 4 and its Subgroups

[65] CIS Control 17 is called "Implement Security Awareness and Training Program"; however, the intent of the control is an institutional-grade training program. CSRIC recommends implementing security training of some form at all levels of organizational cybersecurity maturity.

CIS Control 4: Controlled Use of Administrative Privileges				
#	Asset	Function	Title	Description
4.1	Users	Detect	Maintain Inventory of Administrative Accounts	Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.
4.2	Users	Protect	Change Default Passwords	Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.
4.3	Users	Protect	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.
4.4	Users	Protect	Use Unique Passwords	Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.
4.5	Users	Protect	Use Multi-Factor Authentication for All Administrative Access	Use multi-factor authentication and encrypted channels for all administrative account access.
4.6	Users	Protect	Use Dedicated Workstations For All Administrative Tasks	Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.
4.7	Users	Protect	Limit Access to Script Tools	Limit access to scripting tools (such as Microsoft® PowerShell and Python) to only administrative or development users with the need to access those capabilities.
4.8	Users	Detect	Log and Alert on Changes to Administrative Group Membership	Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.
4.9	Users	Detect	Log and Alert on Unsuccessful Administrative Account Login	Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.

7.7.2 Implementation Groups

The CIS Controls have 20 top-level Controls containing 171 safeguards that provide a prioritized path to gradually improve an organization's cybersecurity posture. To keep current with the evolving threat landscape, CIS defined a new prioritization scheme using Implementation Groups (IGs). An organization can determine what IG they belong to by looking at the sensitivity of the data they need to protect and the resources they can dedicate towards IT and cybersecurity. These IGs are as follows:

- IG1 is the definition of basic cyber hygiene and represents a standard duty of care for all organizations.
- IG2 prescribes what has to be done for more sensitive components of an organization depending upon the services and information they handle.
- IG3 is the highest level of cyber hygiene. These are steps taken for fully mature organizations to protect the most sensitive parts of their missions.

Implementing each IG includes the controls implemented with prior controls; IG2 includes IG1 and IG3 includes IG1 and IG2. Because of the mission-critical nature of 9-1-1 services and the impact a cyber-attack can have on the operations of a 9-1-1 PSAP/ECC, this mapping applies more to the cybersecurity maturity of an organization rather than its size, and thus the mapping relates more to the maturity level of a PSAP/ECC. This maturity level is attributed to the stage in a NG9-1-1 transition, allowing time to properly address the resources necessary to implement each control. The expectation is that PSAPs/ECCs will aggregate into larger entities as the NG9-1-1 transition progresses, and thus the size of the 9-1-1 Agency may also be applicable. The table below suggests a mapping of CIS implementation groups to their 9-1-1 analogs.

Table 5: The Control Groups

CIS Control Group	Description	Commercial Example	9-1-1 Example	Maturity Level
IG1	Cyber-hygiene Basic Security Education	Small Business	Small PSAP/ECC	Legacy Transitional End-State
IG2	Data protection and recovery Network Configuration Boundary Defense	Mid-Size Business	Large PSAP/ECC Regional 9-1-1 Authority	Legacy Transitional End-State
IG3	Institutional Cybersecurity Training Penetration Testing Application Software Security	Large Corporation	Statewide ESInet Core Service Provider	End-State

7.8 Mapping Asset Types to 9-1-1 Domains

Generally, there are five domains involved in the origination and delivery of an emergency call. What happens in each domain changes not only how the entity in the next domain handles the call but can also change which entity handles it. An abbreviated summary of each domain and some examples of which entities or operations fall into that domain is outlined in the table below.

Table 6: The Five 9-1-1 Domains

Originating Device	Originating Service Provider	9-1-1 System	PSAP/ECC	Field Response
Wireline Telephone Mobile device VoIP Terminal Software Client TTY Terminal	ILEC/CLEC PSTN VoIP Provider Cellular Carrier	State/Regional E9-1-1 System State/Regional ESInet Local ESInet Aggregate ESInet	Primary PSAP Secondary PSAP ECC	CAD Police/Fire/EMS Terminals

For the purposes of this analysis, the primary domains considered are the 9-1-1 system and the PSAP / ECC, and to a limited extent, the Field Response domain in as far as it includes systems directly interconnected with the 9-1-1 system, such as CAD systems. These lines become increasingly blurred in a modern world of integrated systems. For example the call-handling and CAD function may employ the same software, operated by the same person, and the field responder mobile terminal accesses the same platform as a web service, and the entire software backend could be hosted in the cloud at the same data center as the NG9-1-1 core services. While acknowledging these complications, this analysis focuses specifically on the 9-1-1 system and ECC domains for the purposes of domain of responsibility for handling emergency calls. The security of other domains is extremely important for the integrity of the broader 9-1-1 system, including and in particular OSP networks. The context of how these other domains interconnect/interact with the 9-1-1 system and PSAPs/ECCs is relevant to the scope of this report.

In the CIS model, these controls apply to five asset types. These types are Users, Devices, Applications, Network and Data. Each sub-control corresponds to an asset type; i.e., a control that requires strong password management is assigned to the "users" asset type that uses these passwords, and a control that requires protection of the organization's information is assigned to the "data" asset type.

7.8.1 Legacy 9-1-1 is Vulnerable to Cyber-Attacks Primarily at the ECC

While a legacy 9-1-1 environment does not handle multimedia inputs from 9-1-1 callers using modern IP technology, it is still vulnerable to attack, such as TDOS attacks, SWATTING, ransomware, and caller identity spoofing. A legacy PSAP, which may use modern technologies and may be connected to the internet, can be compromised through any of the scenarios included in this report—which then harms the ability to handle and respond to 9-1-1 calls. Approximately 70% of all legacy PSAPs/ECCs are small, having 5 or fewer 9-1-1 telecommunicator stations.[66] These smaller Agencies are typically embedded in city and county government infrastructure, and such infrastructures have been under relentless cyber-attacks

[66] See https://www.911.gov/pdf/National-911-Program-Profile-Database-Progress-Report-2019.pdf at pp. 19-20.

over the last few years. Successful attacks have often impaired emergency response, including the disruption of the 9-1-1 call-taking functions. Although operating in a legacy 9-1-1 environment, a legacy PSAP is still a modern enterprise that uses networks, computers and the internet. In some ways, the legacy PSAP represents a disproportionately large vulnerability to cyber-attacks.

Accordingly, even in a legacy 9-1-1 environment, a deep focus on improving the current cybersecurity posture at the legacy PSAP is critical. From a CIS Controls perspective, this means implementing IG1 controls, at a minimum, with an effort to implement IG2 and even IG3 controls if possible.

7.8.2 Transitional 9-1-1 is Vulnerable to Legacy 9-1-1 and End-State NG9-1-1 Attacks

Transitional NG9-1-1 is naturally susceptible to legacy TDOS-style attacks, because it must support legacy origination services and PSAPs but must also support SIP / IP origination and ECCs. In addition, the presence of gateway elements between the legacy elements of the architecture (i.e., originating networks, PSAPs) and ESInets during the transition to end-state NG9-1-1 introduces an expanded Attack Surface with the potential for additional points of vulnerability. Since the transitional architectures described in this report assume the presence of an ESInet as well as the likelihood of one or more legacy PSAPs/ECCs, many of the same attack surfaces apply in a transitional state as in both a legacy state and an end-state NG9-1-1 environment. During transition, the 9-1-1 infrastructure may be considered most vulnerable because it not only includes the attack surfaces of both the legacy and the end-state environment, but also those unique to a transitional architecture. The Transitional State reflects a service that is in transition, whose security controls are still being implemented and upgraded and may not have been tested.

While ideally transitional services should have strong controls to protect against all attacks, by nature of their being transitional services, there needs to be a balance between what is ideal and what is feasible. The greater maturity level of these transitional networks suggests that, from a CIS Controls perspective, implementing IG1 & IG2 controls should be the minimum expectation with IG3 controls being implemented, if possible.

7.8.3 End-State NG9-1-1 Services have Robust Security Features, but a Broad Attack Surface

End-state NG9-1-1 networks include powerful security and resiliency features. For example, a functional element or service in an NG9-1-1 network can communicate, inside or outside of its own ESInet, its security posture indicating that it is operating normally, is under stress or attack or is inoperable.[67] It is required to use strong security mechanisms for protecting data whether stored or in transit[68] , and supports APIs whose payloads cannot be repudiated.[69] These mechanisms, if implemented properly and supported through the ecosystem, provide for a very

[67] See NENA NENA-STA-010.3-2020 at 2.4.1.

[68] See NENA NENA-STA-010.3-2020 at 5.7, 5.8 and 5.9.

[69] See NENA NENA-STA-010.3-2020 at 5.7, 5.8 and 5.10.

high level of baseline security above and beyond a typical enterprise system, which is appropriate for a service like NG9-1-1. NG9-1-1 end state also means that the 9-1-1 ECC can receive multimedia inputs from a 9-1-1 "caller", and this introduction adds a new Attack Surface to the 9-1-1 ecosystem that will rely even more heavily on the end-to-end cybersecurity controls that an NG9-1-1 End State system is expected to have implemented. This NG9-1-1 End State represents the highest maturity level and, from a CIS Controls perspective, implementing all controls through IG3 should be the general practice.

7.9 Guidelines for Implementing Controls through the Transition

The following sections include some general guidelines for which controls can improve the cybersecurity posture of 9-1-1 in a legacy, transitional and end-state NG9-1-1 environment.

7.9.1 All Organizations Should Strive to Achieve All Sub-controls

Ideally every aspect of 9-1-1 service should be secure and resilient, with every part of the service available 100% of the time, immune to cyber-attacks of any kind. However, it is not reasonable to expect that every 9-1-1 organization will have the resources to achieve a strong cybersecurity posture. Even though 9-1-1 is critically important to the safety of life and property in the United States, the stark reality is that not every participant in the 9-1-1 community has sufficient expertise, funding or executive support, and every organization has a different quality of networks, devices and applications that comprise their 9-1-1 service.

ALL organizations should strive to implement ALL sub-controls, and full compliance with IG3 is the ideal end-state for the organization, even if it seems infeasible for the organization. While some of the controls in IG3 are not feasible for all smaller organizations (such as sub-control 1.2, use of a passive asset discovery tool that automatically updates the organization's hardware and software library), some controls are relatively easy to implement even for a small organization (such as two-factor authentication).

Even small organizations should conduct either internal or external security audits, and the audits should record where the organization stands in terms of whether it conforms to security controls or not. They should do this even if initial goals are relatively modest; even if the intent is only to meet IG1, the organization should still plan to make progress towards IG2 in its next cycle. Not only does this provide the organization with a continuous improvement plan to motivate personnel internally to improve procedural and technical controls, it also provides justification in the next budget cycle when trying to secure adequate funding to improve the organization's cybersecurity posture.

7.9.2 Support for IG1, Regardless of Size, Particularly in a Legacy Environment

IG1 includes basic cybersecurity practices that apply to all organizations; basic requirements like maintaining an asset inventory or password management, and basic security training for personnel are reasonable requirements to apply to all organizations. Thus, IG1 applies to small PSAPs/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 generally inexpensive and do not require sophisticated technical resources or systems to implement. 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 Use Cases 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.

The table below shows the controls that can be implemented for all organizations, with a particular focus on immediately implementing them in a legacy 9-1-1 environment, most of which are from IG1:

Table 7: Cybersecurity Controls Applicable to a Legacy 9-1-1 Environment

Control #	Control Title
1.4	Maintain Detailed Asset Inventory
1.6	Address Unauthorized Assets
2.1	Maintain Inventory of Authorized Software
2.2	Ensure Software is Supported by Vendor
2.6	Address unapproved software
3.4	Deploy Automated Operating System Patch Management Tools
3.5	Deploy Automated Software Patch Management Tools
4.2	Change Default Passwords
4.3	Ensure the Use of Dedicated Administrative Accounts
5.1	Establish Secure Configurations
6.2	Activate Audit Logging[70]
7.1	Ensure Use of Only Fully Supported Browsers and Email Clients
7.7	Use of DNS Filtering Services
8.2	Ensure Anti-Malware Software and Signatures Are Updated
8.4	Configure Anti-Malware Scanning of Removable Devices
8.5	Configure Devices to Not Auto-Run Content
9.4	Apply Host-Based Firewalls or Port-Filtering[71]
10.1	Ensure Regular Automated Backups
10.2	Perform Complete System Backups
10.4	Protect Backups
10.5	Ensure All Backups Have at Least One Offline Backup Destination
11.4	Install the Latest Stable Version of Any Security-Related Updates on All Network Devices
12.1	Maintain an Inventory of Network Boundaries
12.4	Deny Communication Over Unauthorized Ports
13.1	Maintain an Inventory of Sensitive Information
13.2	Remove Sensitive Data or Systems Not Regularly Accessed by Organization
13.6	Encrypt Mobile Device Data

[70] Logging is a long-established concept in 9-1-1; calls and dispatch events have long been logged and timestamped for legal purposes.

[71] Though firewalls are diminishing in practical utility in a modern world, it is common practice to implement firewalls the ingress and egress of ESInets.

14.6	Protect Information Through Access Control Lists
15.7	Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data
15.10	Create Separate Wireless Network for Personal and Untrusted Devices
16.8	Disable Any Unassociated Accounts
16.9	Disable Dormant Accounts
16.11	Lock Workstation Sessions After Inactivity
17.3	Implement a Security Awareness Program
17.5	Train Workforce on Secure Authentication
17.6	Train Workforce on Identifying Social Engineering Attacks
17.7	Train Workforce on Sensitive Data Handling
17.8	Train Workforce on Causes of Unintentional Data Exposure
17.9	Train Workforce Members on Identifying and Reporting Incidents
19.1	Document Incident Response Procedures
19.3	Designate Management Personnel to Support Incident Handling
19.5	Maintain Contact Information For Reporting Security Incidents
19.6	Publish Information Regarding Reporting Computer Anomalies and Incidents

7.9.3 Support for IG2 and a Subset of IG3 Controls in Transitional NG9-1-1 Networks

IG2 is intended to provide guidance for modern IP systems of medium to large size. In a commercial setting, these recommendations are in-scope for a company of a few hundred or a few thousand people. As specified above, all organizations should attempt to fulfill the full set of controls. However, transitional networks should exercise *at least* all of the controls in IG2, in addition to those specified for IG1.

These controls tend to be characterized as more modern, enterprise-level controls, and are generally either technical controls or are procedural controls that are more administratively burdensome than the controls included in IG1. For example, the controls include technical controls like automated vulnerability scanning and DNS query logging, or procedurally burdensome controls like regularly reviewing logs.

The table below includes the controls that are applicable to transitional networks, *in addition to every control from the previous section.*

Table 8: Controls Applicable to for a Transitional Environment

Control #	Control Title
1.1	Utilize an Active Discovery Tool
1.3	Use DHCP Logging to Update Asset Inventory
1.5	Maintain Asset Inventory Information
1.7	Deploy Port Level Access Control
2.3	Utilize Software Inventory Tools
2.4	Track Software Inventory Information
2.10	Physically or Logically Segregate High Risk Applications[72]
3.1	Run Automated Vulnerability Scanning Tools
3.2	Perform Authenticated Vulnerability Scanning

[72] 9-1-1 needs necessarily require physical or logical isolation of some systems, even in a legacy environment. End-state NG9-1-1 systems have a degree of logical separation built into the architecture.

3.3	Protect Dedicated Assessment Accounts
4.1	Maintain Inventory of Administrative Accounts
4.4	Use Unique Passwords
4.5	Use Multi-Factor Authentication for All Administrative Access[73]
4.7	Limit Access to Script Tools
4.8	Log and Alert on Changes to Administrative Group Membership
4.9	Log and Alert on Unsuccessful Administrative Account Login
5.2	Maintain Secure Images
5.3	Securely Store Master Images
5.4	Deploy System Configuration Management Tools
5.5	Implement Automated Configuration Monitoring Systems
6.1	Utilize Three Synchronized Time Sources[74]
6.3	Enable Detailed Logging[75]
6.4	Ensure Adequate Storage for Logs
6.5	Central Log Management[76]
6.6	Deploy SIEM or Log Analytic Tools
6.7	Regularly Review Logs
7.2	Disable Unnecessary or Unauthorized Browser or Email Client Plugins
7.3	Limit Use of Scripting Languages in Web Browsers and Email Clients
7.4	Maintain and Enforce Network-Based URL Filters
7.5	Subscribe to URL-Categorization Service
7.6	Log All URL requester
7.8	Implement DMARC and Enable Receiver-Side Verification
7.9	Block Unnecessary File Types
8.1	Utilize Centrally Managed Anti-malware Software
8.3	Enable Operating System Anti-Exploitation Features/Deploy Anti-Exploit Technologies
8.6	Centralize Anti-Malware Logging
8.7	Enable DNS Query Logging
8.8	Enable Command-Line Audit Logging
9.1	Associate Active Ports, Services, and Protocols to Asset Inventory
9.2	Ensure Only Approved Ports, Protocols, and Services Are Running
9.3	Perform Regular Automated Port Scans
9.5	Implement Application Firewalls[77]
10.3	Test Data on Backup Media
11.1	Maintain Standard Security Configurations for Network Devices
11.2	Document Traffic Configuration Rules
11.3	Use Automated Tools to Verify Standard Device Configurations and Detect Changes
11.5	Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions[78]
11.6	Use Dedicated Machines For All Network Administrative Tasks
11.7	Manage Network Infrastructure Through a Dedicated Network

[73] NG9-1-1 standards require MFA for identify providers and otherwise strongly encourage that all accounts are protected by MFA.

[74] GPS clocks and authoritative time are well-established concepts even in legacy 9-1-1, where log records are auditable and timestamps used as evidence in legal proceedings.

[75] Logging is a long-established concept in 9-1-1; calls and dispatch events have long been logged and timestamped for legal purposes.

[76] NG9-1-1 provides for a permissions-based interoperable logging service that is used more or less in real-time in communications during an incident. Security and interoperability are managed through a standardized trust framework. Logging in this case refers to server logs, not incident logs.

[77] Though firewalls are diminishing in practical utility in a modern world, it is common practice to implement firewalls at the ingress and egress of ESInets.

[78] In end-state NG9-1-1, all communications are protected by TLS.

12.2	Scan for Unauthorized Connections Across Trusted Network Boundaries
12.3	Deny Communications With Known Malicious IP Addresses[79]
12.5	Configure Monitoring Systems to Record Network Packets
12.6	Deploy Network-Based IDS Sensors
12.8	Deploy NetFlow Collection on Networking Boundary Devices
12.11	Require All Remote Login to Use Multi-Factor Authentication
13.4	Only Allow Access to Authorized Cloud Storage or Email Providers
13.7	Manage USB Devices
14.1	Segment the Network Based on Sensitivity
14.2	Enable Firewall Filtering Between VLANs
14.3	Disable Workstation to Workstation Communication[80]
14.4	Encrypt All Sensitive Information in Transit
15.1	Maintain an Inventory of Authorized Wireless Access Points
15.2	Detect Wireless Access Points Connected to the Wired Network
15.3	Use a Wireless Intrusion Detection System
15.6	Disable Peer-to-Peer Wireless Network Capabilities on Wireless Clients[81]
16.1	Maintain an Inventory of Authentication Systems
16.2	Configure Centralized Point of Authentication
16.3	Require Multi-Factor Authentication
16.4	Encrypt or Hash all Authentication Credentials
16.5	Encrypt Transmittal of Username and Authentication Credentials
16.6	Maintain an Inventory of Accounts
16.7	Establish Process for Revoking Access
16.10	Ensure All Accounts Have An Expiration Date
17.1	Perform a Skills Gap Analysis[82]
17.2	Deliver Training to Fill the Skills Gap[83]
17.4	Update Awareness Content Frequently
18.1	Establish Secure Coding Practices[84]
18.2	Ensure That Explicit Error Checking is Performed for All In-House Developed Software
18.3	Verify That Acquired Software is Still Supported
18.4	Only Use Up-to-Date and Trusted Third-Party Components
18.5	Use Only Standardized and Extensively Reviewed Encryption Algorithms
18.6	Ensure Software Development Personnel are Trained in Secure Coding
18.7	Apply Static and Dynamic Code Analysis Tools
18.8	Establish a Process to Accept and Address Reports of Software Vulnerabilities
18.9	Separate Production and Non-Production Systems
18.10	Deploy Web Application Firewalls
18.11	Use Standard Hardening Configuration Templates for Databases
19.2	Assign Job Titles and Duties for Incident Response
19.4	Devise Organization-wide Standards for Reporting Incidents

[79] NG9-1-1 creates a trusted environment, so most transactions are assumed to be malicious unless proven to be trustworthy ahead of time.

[80] While a feasible and reasonable expectation for normal IT systems, NG9-1-1 systems require interoperability between agents that constitutes lateral communication within and across the organization. NG9-1-1 provides for special security controls to accommodate this.

[81] While feasible and practical for business networks, some public safety functions, including MCPTT, require some support for peer-to-peer wireless communications between clients. These functions should work within a framework suitable for NG9-1-1's mission.

[82] All organizations of all sizes and implementation phases should perform basic cybersecurity training.

[83] All organizations of all sizes and implementation phases should perform basic cybersecurity training.

[84] The 9-1-1 community does not develop a tremendous amount of software in-house; however, when procuring services, 9-1-1 entities should require their providers to document their adherence to these controls.

19.7	Conduct Periodic Incident Scenario Sessions for Personnel
20.1	Establish a Penetration Testing Program[85]
20.2	Conduct Regular External and Internal Penetration Tests
20.4	Include Tests for Presence of Unprotected System Information and Artifacts
20.5	Create Test Bed for Elements Not Typically Tested in Production
20.6	Use Vulnerability Scanning and Penetration Testing Tools in Concert
20.8	Control and Monitor Accounts Associated with Penetration Testing

7.9.4 Support for IG3 Controls in End-State NG9-1-1 Networks

End-state NG9-1-1 services cannot compromise on security at any portion of the service architecture, and even in the case that calls are originated, handled and delivered in a manner consistent with NG9-1-1, the service should not be considered end-state until *all* elements of the service architecture have achieved a high level of security.

In end-state NG9-1-1, many ESInet operators expose many web services to many other entities that are part of the NG9-1-1 system; for example, the i3 standard describes hundreds of interactions that are available to an endpoint to execute a location and/or routing query[86], retrieving information from an agency's own logger or a logger operated by another agency one is authorized to query,[87] or reporting errors when any of these interactions do not behave as expected,[88] as well as many others. These are all powerful and necessary functions for 9-1-1 entities to interoperate, and when implemented with all security controls, can help ensure 9-1-1 systems and users communicate safety and securely.

However, each of these interactions represents a vulnerability unique to emergency services, because these are interfaces and protocols unique to NG9-1-1. Accordingly, end-state NG9-1-1 has very high security demands; there can be no compromise, and every domain—the caller's device, the OSP, the 9-1-1 system operator and the ECC—must conform with this security regime.

To provide guidance for achieving a high level of security appropriate for end-state NG9-1-1, *all* portions of an end-state NG9-1-1 system should support at least IG3 controls. The applicable controls are included in the table below, *in addition to every control from the previous section.*

Table 9: Controls Applicable to an End-State Environment

Control #	Control Title
1.2	Use a Passive Asset Discovery Tool
1.8	Utilize Client Certificates to Authenticate Hardware Assets[89]
2.5	Integrate Software and Hardware Asset Inventories
2.7	Utilize Application Whitelisting
2.8	Implement Application Whitelisting of Libraries
2.9	Implement Application Whitelisting of Scripts

[85] In general, all members of the 9-1-1 community should exercise their systems, particularly in an end-state NG9-1-1 environment. While normally not a reasonable requirement for small businesses, even a small ECC must be required to demonstrate that they are reputable, trustworthy members of the overall disaggregated NG9-1-1 system.

[86] See NENA NENA-STA-010.3-2020 at 4.3.

[87] See NENA NENA-STA-010.3-2020 at 4.13.

[88] See NENA NENA-STA-010.3-2020 at 3.7.

[89] In NG9-1-1 i3, certificates are required to express credentials traceable to a shared root with ID and role.

2.10	Physically or Logically Segregate High Risk Applications
4.6	Use Dedicated Workstations For All Administrative Tasks[90]
6.8	Regularly Tune SIEM
7.10	Sandbox All Email Attachments
9.5	Implement Application Firewalls
12.7	Deploy Network-Based Intrusion Prevention Systems
12.9	Deploy Application Layer Filtering Proxy Server
12.12	Manage All Devices Remotely Logging into Internal Network
13.3	Monitor and Block Unauthorized Network Traffic
13.5	Monitor and Detect Any Unauthorized Use of Encryption
13.8	Manage System's External Removable Media's Read/Write Configurations
13.9	Encrypt Data on USB Storage Devices
14.5	Utilize an Active Discovery Tool to Identify Sensitive Data
14.7	Enforce Access Control to Data Through Automated Tools
14.8	Encrypt Sensitive Information at Rest
14.9	Enforce Detail Logging for Access or Changes to Sensitive Data
15.4	Disable Wireless Access on Devices if Not Required
15.5	Limit Wireless Access on Client Devices
15.8	Use Wireless Authentication Protocols That Require Mutual, Multi-Factor Authentication
16.13	Alert on Account Login Behavior Deviation
18.4	Only Use Up-to-Date and Trusted Third-Party Components
19.8	Create Incident Scoring and Prioritization Schema
20.3	Perform Periodic Red Team Exercises
20.7	Ensure Results from Penetration Test are Documented Using Open, Machine-readable Standards

As stated several times in this section, ideally, everything in 9-1-1 should be absolutely secure and 100% available because 9-1-1 is a live-saving service. However, it is not reasonable to expect that every entity in the 9-1-1 community will achieve a high level of security overnight or over the same timescale—much like various jurisdictions move forward in the NG9-1-1 transition at different times and at different rates.

The CIS controls provide a convenient, logical approach to improving the cybersecurity posture of organizations in phases that are largely conformant with prevailing security gaps in a legacy, transitional and end-state NG9-1-1 environment. This section considers guidelines for organizations at each stage of the transition, with the ultimate goal of all entities participating in an end-state NG9-1-1 environment and also operating with a very high level of security. This section describes controls that apply to small 9-1-1 organizations with limited resources as well as controls applicable to large and well-resourced organizations responsible for operating secure NG9-1-1 services. If every 9-1-1 organization makes even small improvements, 9-1-1 as a whole will operate more securely and benefit the American public.

[90] NG9-1-1 provides for a trust framework that allows an elevated level of privilege for all trusted members of the NG9-1-1 community. Accordingly, this requirement should apply all the way through the ecosystem.

8 CONCLUSIONS

As also noted in the first report from TFOPA WG1, and reiterated by this CSRIC report, "A lack of cybersecurity poses a clear and present danger to the ECC and emergency communications system(s) in the United States. Creation of some core services, which provide single points of contact, direct reporting, awareness, and data sharing, and real time response to cyber-attacks at multiple levels of government is essential to the success of our efforts to defend next generation networks and systems. The actors, vectors, and outcomes for cyber-attacks against public safety vary widely."[91]

Based upon the above TFOPA observations the Public Safety community approach to 9-1-1 cybersecurity should include:

- A Public / Private Collaboration dedicated to a comprehensive cybersecurity approach.
- The cooperation of the multiple levels of public safety (local, regional, State and Federal) in a number of different ways, both operational and financial.
- An environment that identifies threats, explaining why they are of concern, and making recommendations to the affected ECCs as to necessary steps to mitigate the threat.
- A combined approach to sharing threat intelligence, cybersecurity practices for defending legacy 9-1-1 networks and systems, and a bold, cooperative new architecture for the defense of transitional and fully deployed NG9-1-1 networks.

[91] TFOPA WG1: Optimal Cybersecurity Approach for PSAPs, Final Report, dated December 10, 2015, p. 45

9 Recommendations

In addition to the recommendations presented below there are a separate set of recommendations that accompany each specific use case in Section 7.

- Use Case #1 - Distributed Denial of Service (DDOS) Attack - DNS Amplification Vector
- Use Case # 2 - Telephony Denial of Service (TDOS) Attack
- Use Case #3: SWATTING attack.
- Use Case #4: Ransomware attacks on the public sector
- Use Case #5: Data Privacy Exposure by Extraction
- Use Case #6: Insider Threats

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

- Implementing the appropriate industry-recognized cybersecurity controls in their entirety where possible, and in phases if necessary during the transition;
- Organizations implement basic security controls, regardless of size, in a legacy environment; and
- NG9-1-1 networks implement foundational security controls and some of the organizational security controls;
- Implement Best Practices as indicated in Report 2 and Report 3.

CSRIC VII also provides recommendations to the Commission for future initiatives:

- Review and revise this report to accommodate changes in cybersecurity advancements, improving on the security recommendations for 9-1-1 systems;
- Review cybersecurity aspects of future technologies impacting Public Safety:
    - 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,
    - and other cybersecurity topics as they become known.

Appendix A– PKI

Use of PKI and methods to establish an all TLS environment in NG9-1-1

Industry has made great strides in how they protect data both in transit and at rest. However, as with all things technical, progress means adapting to newer, and hopefully better, ways of achieving security in emerging environments. With the advent of IP based NG9-1-1 systems, it becomes increasingly important to ensure secure transactions. While we are not recommending a specific vendor, or approach, there are several alternatives that should be considered when attempting to define the optimal approach to authentication and verification between ECCs. The goal should be to drive a robustly competitive environment for industry to offer innovative solutions that meet the needs of 9-1-1 professionals such as those specific in properly devised requests for proposals. Examples include public utilities,[92] aviation,[93] the cable modem industry,[94] SHAKEN/STIR,[95] The US Federal Bridge Certification Authority (FCBA)[96] and NENA's i3 specification includes an example of an NG9-1-1 PKI.[97]

While the general public internet employs what equates to a global PKI with several hundred roots, certain special purpose applications may be more effectively served via a specialized PKI or with alternative implementations that encompass a Decentralized PKI (DPKI), examples of which will be discussed later.

(continued)

[92] See, e.g., IEEE recommendations for Smart Grid PKI at https://ieeexplore.ieee.org/document/6102327

[93] See, e.g. the System Wide Information Management (SWIM) Program IAM at https://www.faa.gov/air_traffic/technology/swim/. SWIM is a National Airspace System (NAS)-wide information system that supports Next Generation Air Transportation System (NextGen) goals.

[94]The cable modem industry's PKI is administered by the non-profit organization CableLabs. See https://www.cablelabs.com/resources-archive/digital-certificate-issuance-service

[95] The Secure Telephone Identity Governance Authority oversees the PKI for SHAKEN.

[96] See https://fpki.idmanagement.gov/ca/.

[97] NENA i3 standard establishes some baseline requirements for an NG9-1-1 PKI; see https://www.nena.org/page/i3_Stage3.

What is a PKI?

A PKI is used to establish trust between entities. . This allows any two entities within the PKI to communicate securely without any prior special coordination.

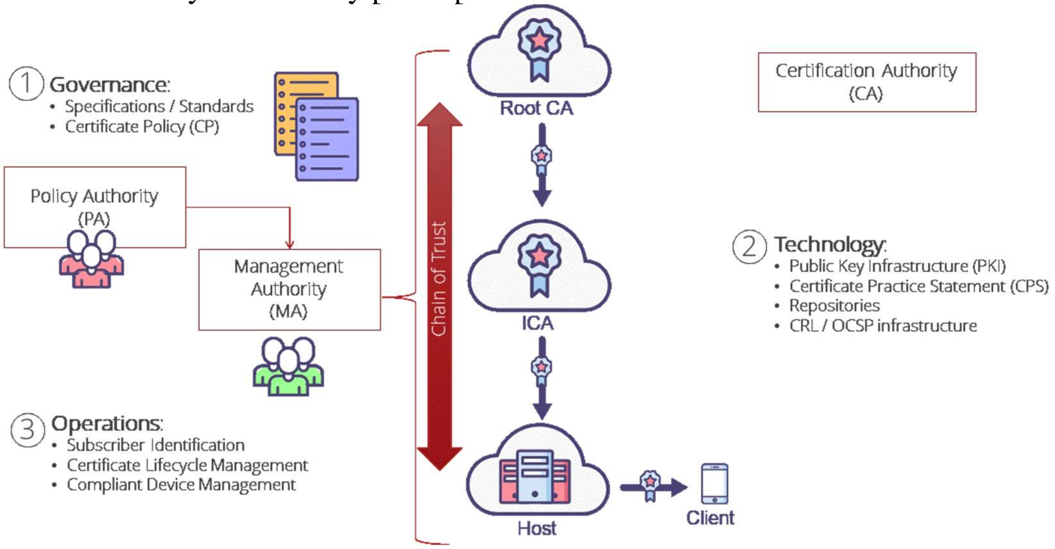

1 Governance:
• Specifications / Standards
• Certificate Policy (CP)
Policy Authority (PA)
Management Authority (MA)
3 Operations:
• Subscriber Identification
• Certificate Lifecycle Management
• Compliant Device Management
Chain of Trust
Root CA
ICA
Host
Client
Certification Authority (CA)
2 Technology:
• Public Key Infrastructure (PKI)
• Certificate Practice Statement (CPS)
• Repositories
• CRL / OCSP infrastructure

Figure A-1: A basic PKI

A PKI is not, from a purely technical perspective, unique. Its security function is identical to the one used on the public internet, in that it involves hosts receiving identity certificates to establish secure connections, such as through Transport Layer Security (TLS) ubiquitous on the internet used for HTTPS. A PKI works in the same manner as the certificate issuing process does for the general public internet. An abbreviated description of the trust chain for the public internet is as follows:

1. Industry necessarily promotes the formation of an entity to become a trusted certificate authority.
2. That party signs a root certificate and it is distributed throughout the trust chain (in the case of the public internet, the root certificate is pre-installed in major browsers)
3. That party distributes identity certificates to hosts, upon request by the host and after verifying the host's identity (e.g., when making a web site the administrator will buy a certificate from a provider for the domain name)
4. That host can now establish a secure session through TLS with any client that has its root certificate
5. The CA, among other things, operates a Certificate Revocation List (CRL), which is distributed through the trust chain to identify which certificates are no longer valid

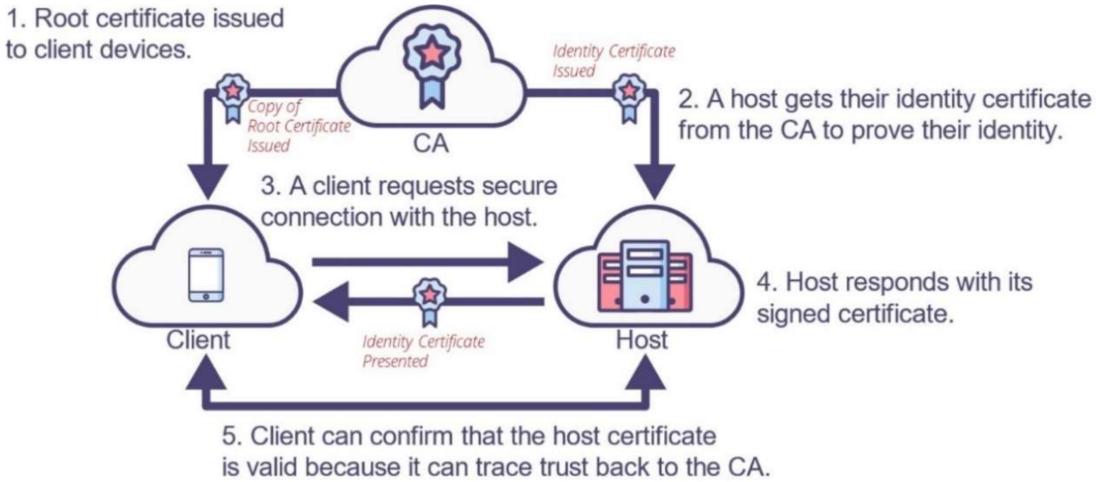

1. Root certificate issued
to client devices.
Copy of
Root Certificate
Issued
CA
Identity Certificate
Issued
2. A host gets their identity certificate
from the CA to prove their identity.
3. A client requests secure
connection with the host.
Client
Host
Identity Certificate
Presented
4. Host responds with its
signed certificate.
5. Client can confirm that the host certificate
is valid because it can trace trust back to the CA.

Figure A-2: Certificate Issuance and Establishing a Secure Connection

The Trust Chain

The trust chain for a PKI, from a technical perspective, works the same as the trust chain for the internet. The difference with a PKI is that it limits membership only to entities within a specified trust chain. For the public internet, any entity can secure a certificate for any domain; that is because the objective of the trust chain for the internet is only to identify ownership of a domain, and anybody can register a domain. However, SHAKEN/STIR, for example, is a PKI. Its trust chain is limited to telecommunications carriers. For a smart grid, that trust chain is limited to the smart devices that are part of the smart grid. For an NG9-1-1 PKI, that trust chain is limited to 9-1-1 entities.

This constraint on participation in the trust chain is the key aspect of a PKI that makes it work. There is a great deal of security that is achieved in establishing a PKI; elements within the PKI can simply ignore any traffic coming from an entity outside of the PKI, which greatly reduces the scope of threat vectors exposed to it. A PKI for NG9-1-1 in turn can ignore any 9-1-1 traffic coming from a source that cannot assert its identity as traceable to the root of trust for NG9-1-1. This is important for NG9-1-1, where emergency call-handling elements are potentially exposed to any entity with an internet connection. In E9-1-1, attacks to the 9-1-1 call-handling system itself are, in many aspects, limited to those elements which can receive a telephone call, because the 9-1-1 call-handling system is designed to handle telephone calls. With the exponentially larger number of devices that can initiate an emergency call in an NG9-1-1 environment, and the similar increased methods of communications these devices can engage in, the NG9-1-1 system may be exposed to an attendant increase in threat vectors. While a PKI does not completely insulate its members from threats, it certainly does protect from a great number of them. However, as there remain inherent risks in the PKI approach, the inclusion of a robust IDPS (such as that proposed in the form of the EC3) should also be considered as a holistic approach to ensure full scope protection.

We note that a rigorous process for establishing membership within a PKI is at the heart of the PKI functioning well; indeed, a specific PKI would establish membership within the 9-1-1 industry, and accordingly grants certain privileges to anyone granted credentials within it. Accordingly, CSRIC VII also recommends that 9-1-1 authorities ensure, through their procurement practices, that their prospective vendors establish a rigorous process, with strong oversight, that enables the 9-1-1 authority to vet any individual granted credentials within any NG9-1-1 PKI.

Root CAs and ICAs

Typically, in a PKI, the system consists of a Root CA and Issuing CAs (ICAs). The Root CA has only one purpose: it signs ICAs. ICAs, in turn, issue identity certificates. In the NG9-1-1 PKI, CSRIC envisions that ICAs could be run by a variety of entities; a state 9-1-1 authority may operate an ICA to credential elements within its NG9-1-1 network, or a service provider may operate an ICA and integrate it into their product offering, managing all of the credentialing on the public safety customer’s behalf. An entity entirely outside what is conventionally considered NG9-1-1 may operate an ICA as it may have special needs to interoperate as a member of the NG9-1-1 PKI. The important role of the ICAs is they actually issue the certificates to end-entities; the Root CA does none of this. In most cases, the root certificate authority server in a PKI is not even connected to the internet. CSRIC makes no specific recommendations as to whom should operate ICAs, whether public or private, or how many of them there should be.

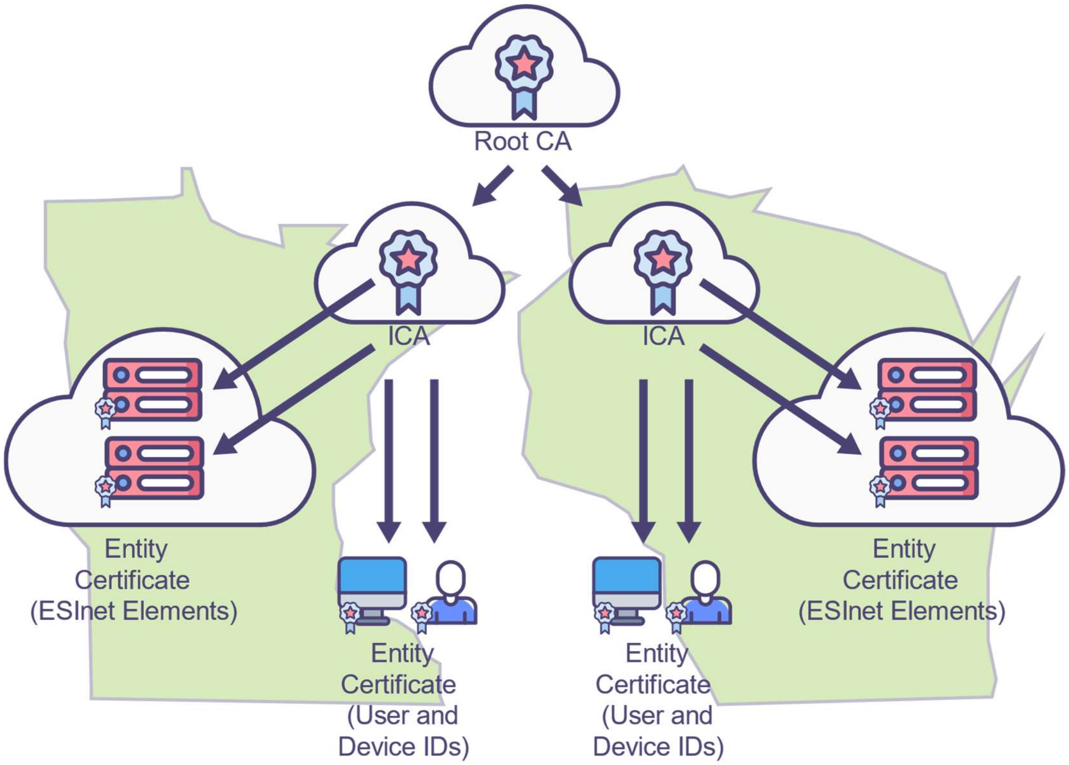

Root CA
ICA
ICA
Entity Certificate (ESInet Elements)
Entity Certificate (User and Device IDs)
Entity Certificate (User and Device IDs)
Entity Certificate (ESInet Elements)

Figure A-3: Trust Chain Depicting two Statewide ICAs under a Root

The Need for Governance in a PKI

Oversight and control are absolutely essential within any PKI; it is more important than any of the technical aspects of any PKI solution. For that very reason every successful PKI has established a strong governance structure so that the PKI can be managed by the stakeholders affected by it. This means that NG9-1-1 vendors must enable 9-1-1 authorities to develop and manage the certificate policy and oversee issuance of certificates and management of the Certificate Revocation List (CRL).

For example, the STIR/SHAKEN framework has a robust governance model in the Secure Telephone Identity Governance Authority (STI-GA), which manages the PKI for using security certificates to authenticate telephone numbers. STI-GA operates under the auspices of ATIS, and is a critical body helping the industry achieve success in mitigating the problem of unwanted robocalling. The STI-GA is defining the rules governing the certificate management infrastructure to ensure effective use and security of SHAKEN certificates. The STI-PA service with approved STI-CAs went live on December 16, 2019.[98]

PKIs in a Transitional Environment

NG9-1-1 faces a series of challenges in the transitional environment that exists while a PKI is

[98] Text taken in part from *Frequently Asked Questions on SHAKEN,* https://www.atis.org/sti-ga/resources/docs/shaken-faqs.pdf

being implemented. End-state NG9-1-1 should have a robust PKI environment where all entities are properly credentialed and share a trust chain. However, there exists a transitional environment where a PKI may exist but not all 9-1-1 entities have joined the trust chain, or the environment today where there may be efforts to deploy a PKI but a mature one does not exist yet.

One substantial case will be that a PKI exists that is used for 9-1-1 in an area, but it has not been integrated into the broader NG9-1-1 PKI. For example, a state or region may have deployed an NG9-1-1 system, and deployed a PKI throughout the entire state, providing interconnectivity within that state. However, it has no interconnectivity with a system that is a member of the broader NG9-1-1 PKI. In this case, it is ideal that the system would eventually join the broader NG9-1-1 PKI. As a transitional measure, however, the regional PKI could cross-sign with the ICA of the NG9-1-1 ESInets of its immediate neighbors providing for some interconnectivity.

Zero Trust Model for NG9-1-1 as a consideration

Zero-trust is built on the concept that a system does not implicitly trust any element inside or outside of it. With a zero-trust framework, there is no “DeMilitarized Zone” (DMZ; In computer security, a DMZ Network [sometimes referred to as a “demilitarized zone”] functions as a subnetwork containing an organization's exposed, outward-facing services and it acts as the exposed point to untrusted networks, like the Internet); everything inside of your network is assumed to be a threat until it can prove that it is not. This applies to two FEs within an ESInet communicating with each other just as much as it does a core services element communicating with an outside originating service provider. Though a zero-trust framework cannot account for all intrusions or compromise of the network, zero-trust means there is no material difference in implicit trust for transactions either inside of outside of the network. Accordingly, compromise of one element means the compromise of only that one element and not the entire system.

There are a number of mechanisms that facilitate communications in a zero-trust environment. Within the context of a PKI, this means confirming membership within the PKI for any element, even if it is inside of your own network. Additionally, zero-trust employs a variety of other practices, such as the least privilege principle, where any element is only provided the minimum amount of access that it needs to do exactly and only what it needs to do, multi-factor authentication (where secondary means in addition to a password are used to authenticate a person, such as a text message), and other means.

Zero-trust could be useful in NG9-1-1 because it is very hard to identify a DMZ in an NG9-1-1 environment; there are not always clear demarcation points to secure, lock down and monitor. Take the example below, which is a simplified diagram of an NG9-1-1 system with many of its key FEs. In a conventional network diagram, core services including the Emergency Services Routing Proxy (ESRP) are within the core services network, and the PSAP FE sits on the outside of the ESInet on the other side of a Border Control Function (BCF). It is quite typical for the PSAP to be a local agency and for the 9-1-1 authority operating the network at a county or regional level. So it is logical to consider a clear demarcation point between the PSAP FE and the core services environment at the BCF, a function expressly designed to define a boundary, and it is logical to depict very clear demarcation points in the NG9-1-1 system.

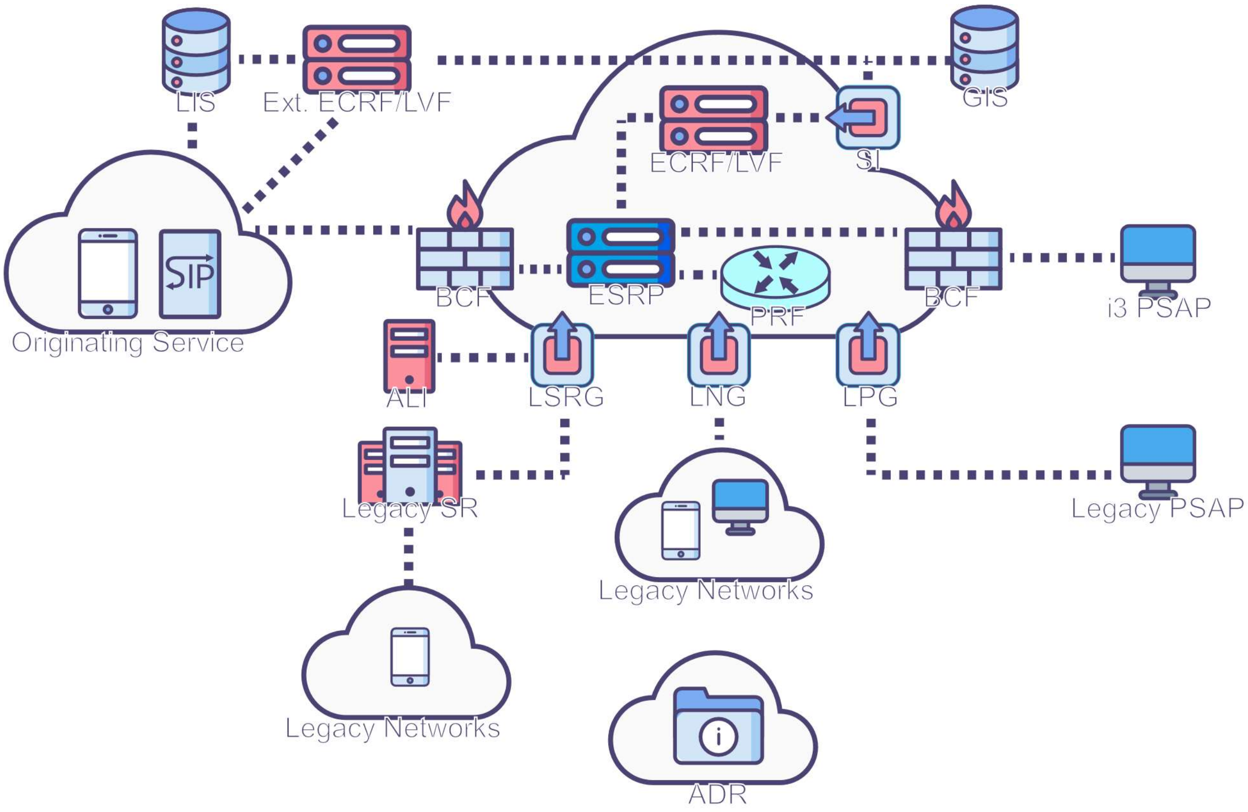


Figure A-4: Simplified NG9-1-1 Network Diagram

However, from a typical developer perspective, there is not necessarily such a clear demarcation point; the developer will make software that queries a variety of web services available to it for whatever it needs to do. It may query a logger to retrieve information in its own network or in someone else's network that it has permission to; there is no difference in inherent trust and the software has to authenticate the same way regardless of where that logger sits. Also, depending on the perspective of the querier, the PSAP web service may out "outside of NG9-1-1" as it sits outside of core services, or it may sit "inside of NG9-1-1-1" because a third-party system or a mobile app used by a field responder is interfacing with it. Again, there is no difference in inherent trust and no concept of a DMZ. This is increasingly complicated with the proliferation of cloud services, where there is no physical demarcation point at all, and an element is simultaneously inside of your core services network and also outside of it.

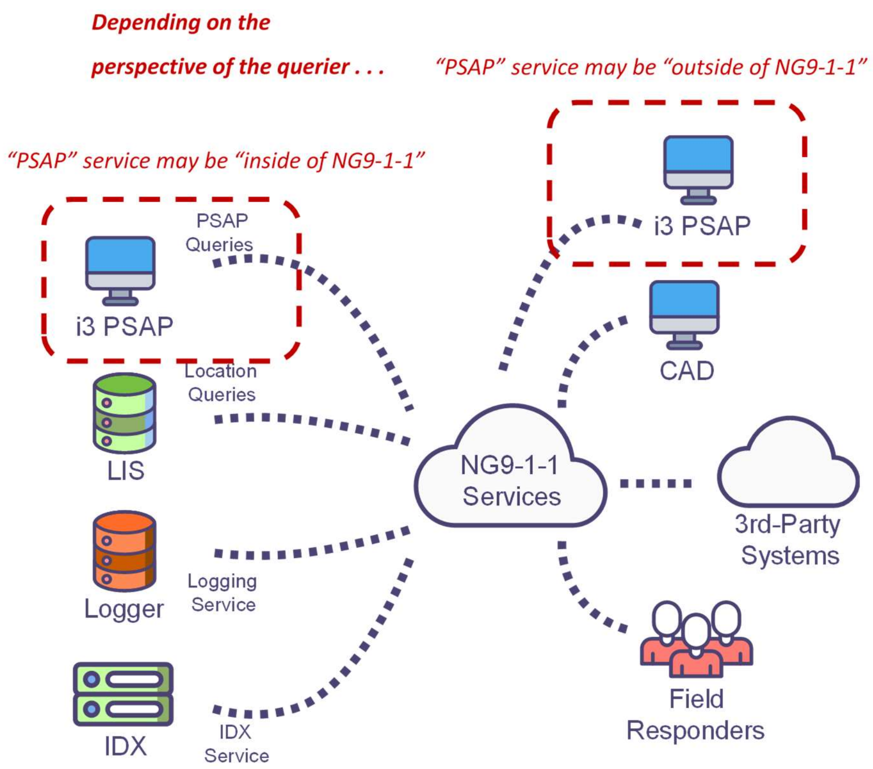


Figure A-5: Queries for Various Services within NG9-1-1

However, while NG9-1-1 provides a lot of capabilities, every single interface available to process any kind of signaling or respond to any query is another attack vector. This makes NG9-1-1 look much more like the modern internet in its function.

Caution regarding Self-Signed Certificates, even Within a DMZ

A self-signed certificate is a certificate signed and issued by the host that presents the certificate; it is a trust chain that does not have a trusted third-party CA at its root. This is a technically easy solution that can establish secure connections between any two endpoints. In the past, self-signed certificates have traditionally been used within closed networks past a DMZ, such as the connection between a web server and backend system. The figure below shows a typical case; there is a host that has a certificate issued by a reputable CA that it presents to any client. However, to save costs and maintenance, the system is configured to self-sign certificates within the DMZ between the host and its backend systems. This maintains security between elements inside of the network because TLS can still be established and saves on costs and maintenance overhead in getting multiple certificates from a reputable CA for multiple elements within the system. The assumption in this design is that since nothing outside of the safe perimeter will talk to the backend system that it is safe to use a self-signed certificate; you need only to have a strong intrusion detection and prevention system to protect the perimeter.

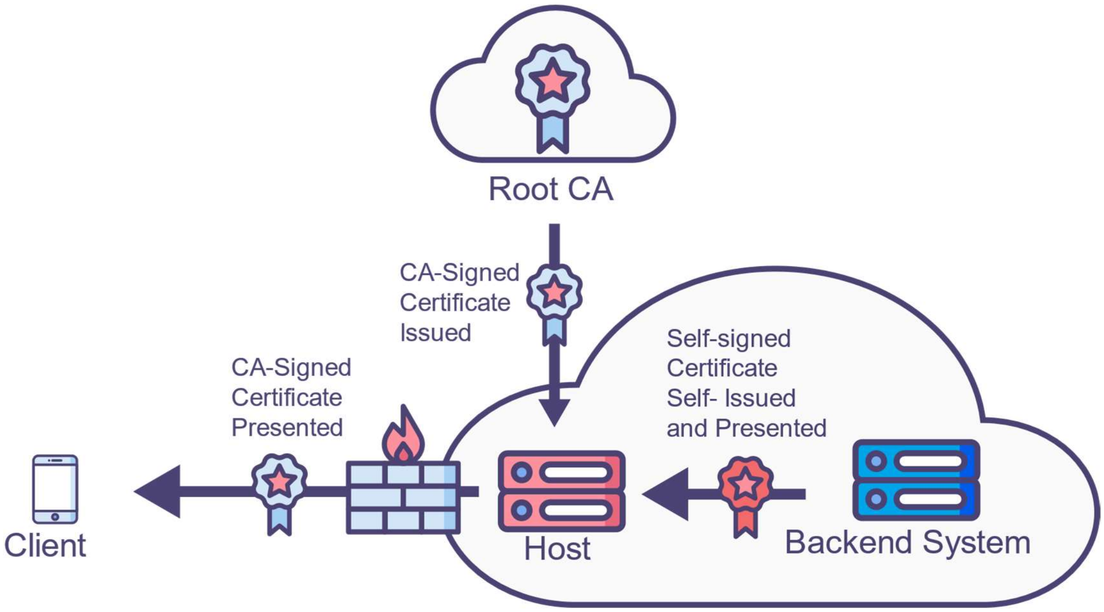

Root CA
CA-Signed Certificate Issued
CA-Signed Certificate Presented
Self-signed Certificate Self- Issued and Presented
Client
Host
Backend System

Figure A-6: Self Signed Certificate Issuance

The security concern with self-signed certificates, even within a heavily protected DMZ, is that if any part of the network is compromised, an intruder may have access to the entire network, because they can then present valid certificates. This is because it can self-sign a certificate that appears valid, because elements in the system don't confirm the validity of the credential with a third party. The figure below demonstrates a very typical man-in-in middle attack that is possible within a DMZ because the network accepts self-signed certificates within its own system. When self-signed certificates are allowed, the client can tell no difference between the above or below figures; the traffic looks legitimate in either case.

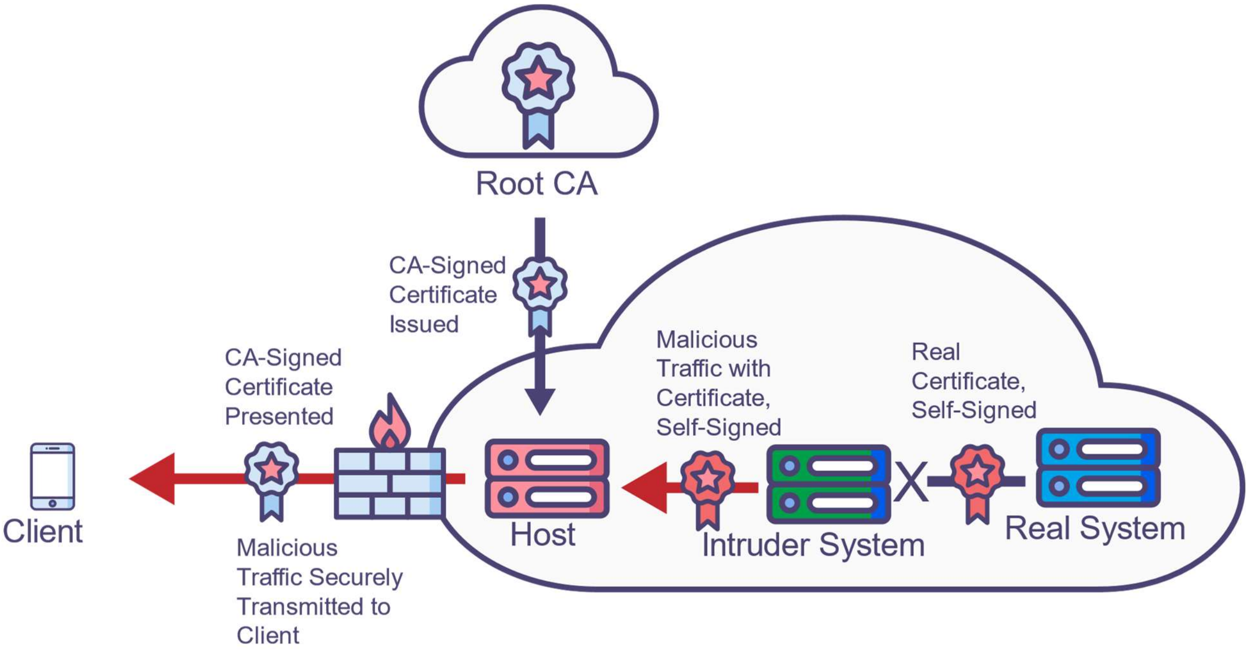

Root CA
CA-Signed Certificate Issued
CA-Signed Certificate Presented
Malicious Traffic with Certificate, Self-Signed
Real Certificate, Self-Signed
Client
Host
Intruder System
X
Real System
Malicious Traffic Securely Transmitted to Client

Figure A-7: Man-in-the-Middle Attack Using Self-Signed Certificates

This type of attack can and has happened. For example, one large root certificate authority in 2011 had an individual compromise their entire network including their certificate issuing servers. In this case the attacker compromised a web server that was within the company's DMZ. Once inside, the intruder was able to compromise all eight of the CA's certificate-issuing servers, including the server that issued government certificates in that country, because elements past the DMZ accepted self-signed certificates and couldn't confirm that part of the network was compromised. The intruder successfully issued valid certificates for a number of high-value domains including *.google.com, Yahoo, Mozilla and others, potentially redirecting any consumer of those services to their server instead of. The root cause of this issue was ruled to be poor enforcement of network rules.[99]

This has clear indications for NG9-1-1. For example, NENA notes that interactions in the i3 specification for NG9-1-1 require establishing TLS using certificates that exist within the NG9-1-1 PKI.[100] It also *requires* that certain transactions are accepted so long as an entity has such a certificate as well. This enhances security of course by defining the scope of a PKI. For example, a PSAP with credentials within the NG9-1-1 can transfer a call to *any other* PSAP, because the transfer-to PSAP must accept any transfer from an entity that can assert its membership within the PKI. Additionally, the PSAP can ignore anything that *looks* like a call transfer if the sender cannot prove it is inside of the PKI—a case that you may see where a bad actor may try to impersonate a PSAP, for example.

[99] See *Report of the investigation into the DigiNotar Certificate Authority Breach, Netherlands Ministry of the Interior and Kingdom Relations, 13 August 2012. Copy retrieved 17 April 2020 from* https://www.researchgate.net/publication/269333601_Black_Tulip_Report_of_the_investigation_into_the_DigiNotar_Certificate_Authority_breach.

[100] See e.g., NENA STA-010 Section 5.

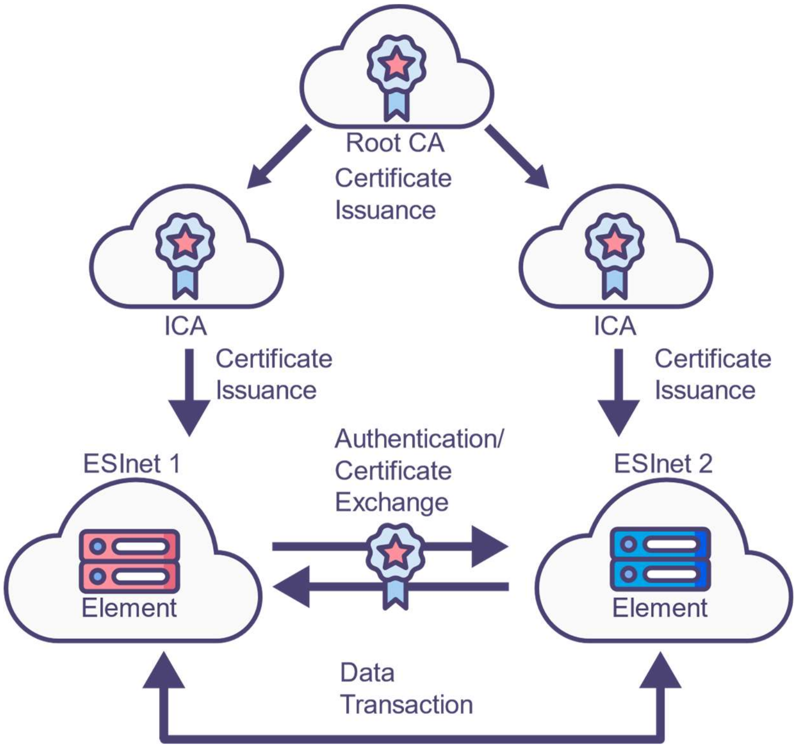


Figure A-8: Participation in a PKI Facilitating Interoperability

Additional considerations

PKI provides a chain of trust so that identities on a network can be verified. However, like any chain, a PKI is only as strong as its weakest link. Below are a variety of citations from industry literature describing alternative means of establishing trust.

“There are various standards that cover aspects of PKI -- such as the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 2527). The Certification Authority Browser Forum, also known as CA/Browser Forum, is an industry consortium founded in 2005 and whose members include CAs, browser software publishers and other system providers who use X.509 digital certificates for encryption and authentication. The CA/Browser Forum publishes guidelines and best practices for CAs, browser and other parties involved in the PKI as it relates to the use of digital certificates.

Although a CA is often referred to as a "trusted third party," shortcomings in the security procedures of various CAs in recent years has jeopardized trust in the entire PKI on which the internet depends. If one CA is compromised, the security of the entire PKI is at risk. For example, in 2011, Web browser vendors were forced to blacklist all certificates issued by the Dutch CA DigiNotar after more than 500 fake certificates were discovered. In 2017, Google engineers identified problems with certificates issued through Symantec's CA business, which led to subsequent distrust of all certificates issued by Symantec prior to the sale of its CA business to DigiCert last year."[101]

"The Internet facilitates communications and transactions between individuals worldwide. This is conducted through the use of identifiers such as email addresses, domains, and usernames. But who controls these identifiers? How are they managed? And how is secure communication facilitated between them? In the modern day, third-parties such as DNS registrars, ICANN, X.509 Certificate Authorities (CAs), and social media companies are responsible for the creation and management of online identifiers and the secure communication between them. Unfortunately, this design has demonstrated serious usability and security shortcomings The answer is not to abandon PKI, but to find an alternative: DPKI, a future specification for a decentralized public-key infrastructure. The goal of DPKI is to ensure that, unlike PKIX, no single third-party can compromise the integrity and security of the system as whole. Trust is decentralized through the use of technologies that make it possible for geographically and politically disparate entities to reach consensus on the state of a shared database. DPKI focuses primarily on decentralized key-value datastores, called blockchains, but it is perfectly capable of supporting other technologies that provide similar or superior security properties. Third-parties, who are called miners (or validators), still exist, but their role is limited to ensuring the security and integrity of the blockchain (or decentralized ledger). These third-parties are financially incentivized by a consensus protocol to follow the rules of the protocol. Deviation from the protocol results in financial punishment, while consistency with the protocol typically results in financial reward. Bitcoin, devised by Satoshi Nakamoto, is the first such successful protocol. Itis based on proof-of-work, in which the energy expenditure of "miners" is used to secure the database"[102]

Simple public key infrastructure

Another alternative, which does not deal with public authentication of public key information, is the simple public key infrastructure (SPKI).

Blockchain-based PKI

An emerging approach for PKI is to use the blockchain technology commonly associated with modern cryptocurrency. Since blockchain technology aims to provide a distributed and unalterable ledger of information, it has qualities considered highly suitable for the storage and management of public keys. [103]

DANE – DNS Based Authentication of Named Entities

Authentication of Domain Name System (DNS) names for Transport-Layer Security (TLS) endpoints is a core security challenge in many Internet protocols, most famously Hypertext Transfer Protocol (HTTP). Today, the cryptographic bindings that underlie TLS authentication

[101] https://searchsecurity.techtarget.com/definition/PKI
[102] https://danubetech.com/download/dpki.pdf
[103] https://en.wikipedia.org/wiki/Public_key_infrastructure#Web_of_trust

are asserted in Public Key Infrastructure for X.509 (PKIX) certificates issued by third-party certification authorities (CAs). The DNS-based Authentication of Named Entities (DANE) working group is developing protocols that allow certificates to be bound to DNS names using Domain Name System Security Extensions (DNSSEC). These protocols will enable additional assurances for the traditional, PKIX-based model, as well as enabling domain holders to assert certificates for themselves, without reference to third-party certificate authorities.[104]

[104] https://www.ietfjournal.org/dane-taking-tls-authentication-to-the-next-level-using-dnssec/

Appendix B – IDPS

Proposed Approach for IDPS in the NG9-1-1 Environment

In the proposed NG9-1-1 architecture, the Emergency Communications Cybersecurity Center (EC3) will take on the role of providing IDPS services to ECCs and any other emergency communications service or system that would consider utilizing the centralized, core services architecture proposed. For example, not only ECCs but Emergency Operations Centers (EOCs) and potentially the Nationwide Public Safety Broadband Network operated and maintained by FirstNet, could also interconnect to the EC3 service. 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.

The potential flow of this system would begin with the Originating Service Provider (OSP) and NG9-1-1 Core Services elements, would encompass the ESInet IP Transport network within and between disparate ECCs and would provide for monitoring of call statistics, system health, anomaly detection, data sharing, mitigation and recovery while still allowing local agencies to maintain local control of day to day operations within their specific ECCs. 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. While not specified herein, the interconnect requirements would include cyber hygiene elements at the ECC, single user sign on and multi-factor authentication at the local level and some form of agreed upon, trusted connection (and relationship) from the local levels to the State or Regional level EC3. This architecture is also intended to represent 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 a centralized repository with adequate service capabilities to support multiple clients, and incidents, in real time. Some examples of how this data flow, and cooperative approach, might present are included in Figures 1 and 2 on the following pages.

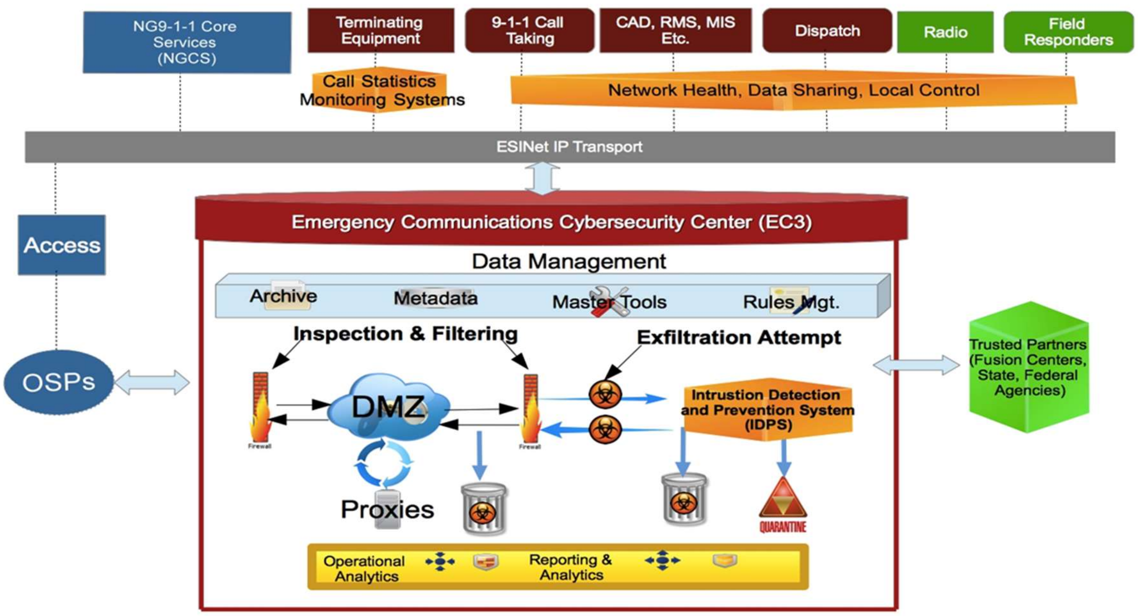


Figure B-1: The Emergency Communications Cybersecurity Center (EC3)

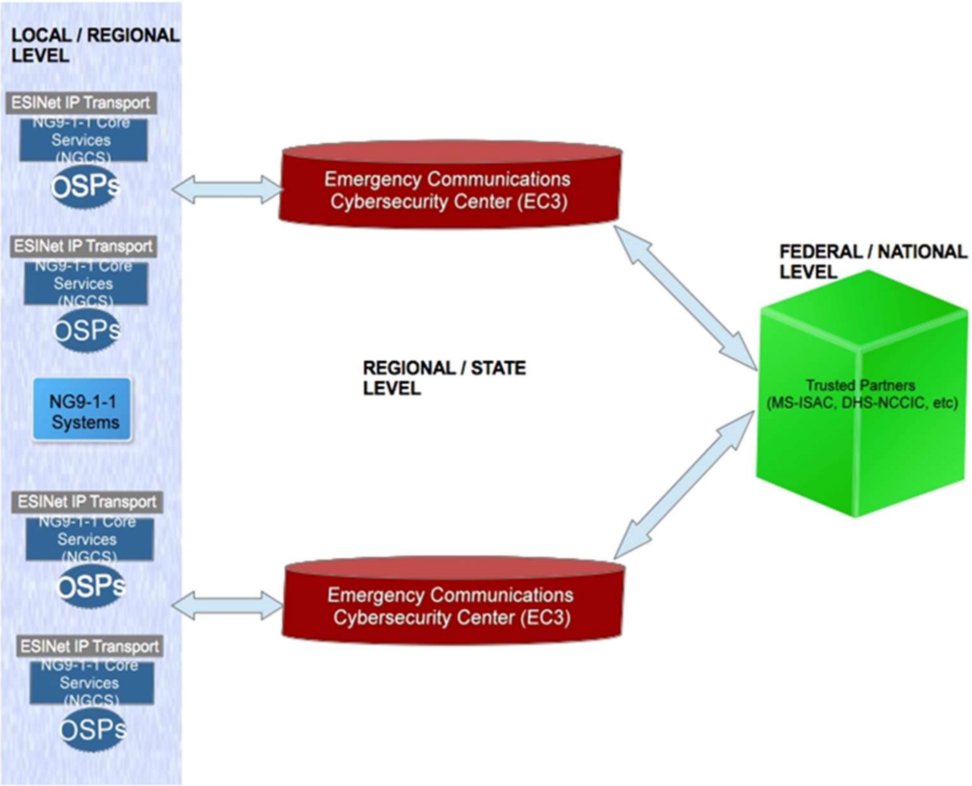

LOCAL / REGIONAL LEVEL
ESINet IP Transport
NG9-1-1 Core Services (NGCS)
OSPs
ESINet IP Transport
NG9-1-1 Core Services (NGCS)
OSPs
NG9-1-1 Systems
ESINet IP Transport
NG9-1-1 Core Services (NGCS)
OSPs
ESINet IP Transport
NG9-1-1 Core Services (NGCS)
OSPs
Emergency Communications Cybersecurity Center (EC3)
REGIONAL / STATE LEVEL
Emergency Communications Cybersecurity Center (EC3)
FEDERAL / NATIONAL LEVEL
Trusted Partners (MS-ISAC, DHS-NCCIC, etc)

Figure B-2: The EC3 Deployed

Operationalizing the EC3 – Options and Opportunities

The EC3 Concept Explained

The information collected by the EC3s that relates to the ECCs will be the result of the monitoring that the center will be doing for them. As a result, it will be necessary to deploy some type of IDS sensors at each ECC location. Alternately, and perhaps more effectively, a way will need to be devised to get all traffic to funnel through a centralized EC3 for monitoring at a regional or State level, then aggregating the traffic of the various EC3's to, or through, a central monitoring facility. This would best be accomplished via the ESInet architecture with partnerships at the Local, State and potentially Federal level.

The type, and location, of deployed sensors should include consideration of both an organization's outermost perimeter, right behind what is handling the organization's network address translation (NAT), and in the case of 9-1-1 traffic the systems feeding information to the 9-1-1 networks. This would potentially include wireless and wireline carrier networks. One option to consider is the use of sensors specifically designed to conduct continuous Netflow monitoring and analysis. The Center for Internet Security (CIS) has deployed such a system, known as Albert, which is an automated process of collecting, correlating, and analyzing computer network security information across State governments. According to CIS, the seven key Netflow fields are: source IP address, destination IP address, source port number, destination port number, protocol type, flags, and the router input interface. While CSRIC VII is not endorsing any specific vendor, product, or organization the model provided by CIS in support of the Multi-State Information Sharing and Analysis Center (MS-ISAC) is a useful model and case study. For the purposes of this report, we will refer to "Albert-like" sensors to define the proposed capabilities. In the case of deployment of "Albert-like" sensors for the data network portion of the solution, CSRIC VII received input and assistance from representatives of the MS-ISAC.[105]

The idea behind the deployment of "Albert-like" sensors is that at some point, an infected system is going to have to reach out to a host on the Internet to receive additional commands, download additional software, or exfiltrate information. Monitoring an organization's Internet connection is an effective way to get visibility into their network. The limitation here is that there may not be good visibility on internal-to-internal communication. This is typically not a concern as most of the attacks and compromises originate from, or beacon out to, the Internet at some point. Setting up the ECCs so that an EC3 would essentially function as their ISP would be an effective way to have eyes on that type of traffic.

In addition to the deployment of "Albert-like" sensors, consideration should be given to a model currently in use by the State of California's Office of Emergency Services (CalOES). This system is comprised of a "phased array" approach with sensors deployed at each ECC in the State that monitor traffic from wireless communications sites. Specifically these sensors, which are currently deployed and actively monitored by both CalOES and the DHS NCCIC, provide a near real time picture of the health and status of every wireless site, and system, responsible for providing wireless connectivity to the public and wireless 9-1-1 traffic to the ECCs.

The mission of the federal government's emergency communications charter (to ensure that relevant federal, state, local, tribal and territorial officials can continue to communicate in the event of a catastrophic loss of communications) can be seen as largely dependent on the federal government's ability to understand mission impacts on emergency communications. It is imperative that this is done in a timely manner so that coordinated response and recovery efforts get to those systems in time. Sensors and business processes, providing visibility into those systems, enabling rapid assimilation of critical emergency communications impacts to state, local and tribal governments by the federal government currently do not exist in an effective manner.

The California Governor's Office of Emergency Services (CalOES) in coordination with NENA and APCO, proposed leveraging an existing sensor system deployed within ECCs in California could be used to support a mission of protecting the ECCs as an enterprise against cyber-attacks, physical disaster response and ensuring continuity of emergency communications.

[105] More information about the MS-ISAC can be found at https://msisac.cisecurity.org.

The sensor system network enables real-time visualization of call data, without any Personally Identifiable Information (PII), which can alert a monitoring center, such as NCCIC, to a disruption to 9-1-1 services by the Local Exchange Carrier, or named wireless service providers, as observed in Virginia during the Derecho, or after an Earthquake. CalOES, in an unprecedented effort to share real-time data with the federal government for disaster management purposes, has developed a demonstration concept with the National Coordination Center for Communications (NCC), which could provide the basis for defending the enterprise of ECCs against emerging cyber threats, or attempts by terrorists to disrupt emergency communications during a coordinated domestic attack against the homeland, or simply improve response coordination to disaster communications restoration after a natural disaster.

As should be obvious to the reader at this point, monitoring of both voice and data networks that feed the 9-1-1 system, and of the data systems within and between ECCs is of great importance and can be accomplished via a combination of mechanisms. In addition to monitoring, mitigation is a key element in the overall function, and goal, of the EC3 concept. The EC3 will likely be tasked with identifying threats, explaining why they are of concern, and making recommendations to the affected ECCs as to necessary steps to mitigate the threat.

Most of what is seen in current Security Operations Centers, such as the MS-ISAC, is tied back to malware infections that can either be cleaned or the systems re-imaged entirely. It will also become important to track any incidents that are escalated to the ECCs in some form of ticketing system for tracking and reporting services. In addition, it would be most effective if there was a method to correlate all the alerts generated by deployed sensors across all EC3s in order to identify any trending related to the top threats facing the ECCs.

Depending on the specific needs of the ECCs, not every EC3 may need to have every service available to it. As an example, computer forensics services may not be a requirement at each EC3. Perhaps only the larger EC3s in the large urban areas throughout the country may have forensics capabilities and the EC3s could coordinate to send forensic images for analysis along to those designated EC3s. Likewise, certain reporting capabilities and aggregate products could be handled by either larger, regional EC3's or even by trusted Federal partners.

Potentially, all of the data from the sensors would route back to the NCCIC and MS-ISAC, or similar facilities, for analysis and escalation back out to the EC3s. As the system continued to build out monitoring infrastructure, it would become easier to correlate data across multiple partners and start to paint the picture of how new attacks and threats evolve as they begin to affect the various SLTT entities being monitored.

As an aside, the MS-ISAC currently has numerous sensors deployed, and hopes to have 41 States on their monitoring service by the end of 2015. In addition, they have an excellent working relationship with the NCCIC with two full-time CIS staff on the NCCIC floor. This allows the NCCIC to provide the MS-ISAC with indicators of compromise that they can then retroactively search for across all of their sensors, or use to create signatures to identify new compromises going forward. As noted, the NCCIC is already engaged in cyber defense of ECCs and critical communications infrastructure and therefore is a logical partner to consider. In addition, the Federal Communications Commission itself has partnered with DHS on multiple fronts and should continue to be actively involved in efforts to understand how we can best design, build, and defend these emergency communications cybersecurity systems as a cooperative effort between public safety and industry.[106]

[106] Appendix B of this document is taken from Sections 6.3 and 6.3.1 of the TFOPA WG1: Optimal Cybersecurity Approach for PSAPs, Final Report, dated December 10, 2015 , pp. 34-40

Appendix C – Best Practices

BP #	Best Practice	Legacy	Transition	End State
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. This applies to Public Safety only in an NG9-1-1 environment.		TRUE	TRUE
12-12-8117	Network Operators, Service Providers and Public Safety should prepare a disaster recovery plan to implement upon DNS server compromise. This applies to Public Safety only in an NG9-1-1 environment.		TRUE	TRUE
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
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, Service Providers and Public Safety should apply caller authentication/verification techniques (e.g., using the SHAKEN framework) to mitigate Caller ID spoofing.		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
12-12-8540	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&~~amp;~~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
12-12-8758	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
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 a network element or server is under DoS attack~~. If it is not a configuration/hardware issue, d~~D~~etermine 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 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 3rd party provider. This applies to Public Safety only in an NG9-1-1 environment.		TRUE	TRUE

12-12-8527	Network Operators, Service Providers and Public Safety should if the DNS (Domain Name System) server has been compromised or the name records corrupted, first flush the DNS cache and, failing that, implement the pre-defined disaster recovery plan. Elements 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
12-12-8517	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
12-12-8130	Network Operators, Service Providers, Equipment Suppliers and Public Safety should provide procedures and training to staff on the reporting of security incidents, weaknesses, and suspicious events.	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	
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

Appendix D - Applying CIS Controls for the NG9-1-1 Transition

CIS Control	Asset Type	Security Function	CIS Sub-Control	Title	Description	Implementation Group 1	Implementation Group 2	Implementation Group 3	Legacy 9-1-1	Transitional	End-State	PSAP/ECC	ESInet	CSRIC Comments
1	Devices	Identify	1.1	Utilize an Active Discovery Tool	Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.		X	X		X	X		X	
1	Devices	Identify	1.2	Use a Passive Asset Discovery Tool	Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory.			X			X		X	
1	Devices	Identify	1.3	Use DHCP Logging to Update Asset Inventory	Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset inventory.		X	X		X	X	X	X	
1	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.	X	X	X	X	X	X	X	X	

1	Devices	Identify	1.5	Maintain Asset Inventory Information	Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network.		X	X		X	X		X	
1	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.	X	X	X	X	X	X	X	X	
1	Devices	Protect	1.7	Deploy Port Level Access Control	Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.		X	X		X	X		X	
1	Devices	Protect	1.8	Utilize Client Certificates to Authenticate Hardware Assets	Use client certificates to authenticate hardware assets connecting to the organization's trusted network.			X			X	X	X	In NG9-1-1 i3, certificates are required to express credentials traceable to a shared root with ID and role.
2	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.	X	X	X	X	X	X	X	X	
2	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.	X	X	X	X	X	X			
2	Applications	Identify	2.3	Utilize Software Inventory Tools	Utilize software inventory tools throughout the organization to		X	X		X	X		X	

					automate the documentation of all software on business systems.									
2	Applications	Identify	2.4	Track Software Inventory Information	The software inventory system should track the name, version, publisher, and install date for all software, including operating systems authorized by the organization.		X	X		X	X		X	
2	Applications	Identify	2.5	Integrate Software and Hardware Asset Inventories	The software inventory system should be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.			X			X		X	
2	Applications	Respond	2.6	Address unapproved software	Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	X	X	X	X	X	X	X	X	
2	Applications	Protect	2.7	Utilize Application Whitelisting	Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.			X			X		X	
2	Applications	Protect	2.8	Implement Application Whitelisting of Libraries	The organization's application whitelisting software must ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc.) are allowed to load into a system process.			X			X		X	
2	Applications	Protect	2.9	Implement Application Whitelisting of Scripts	The organization's application whitelisting software must ensure that only authorized, digitally signed scripts (such as *.ps1, *.py, macros, etc.) are allowed to run on a system.			X			X		X	
2	Applications	Protect	2.10	Physically or Logically Segregate High Risk Applications	Physically or logically segregated systems should be used to isolate and run software that is required for business operations but incurs higher risk for the organization.			X	X	X	X	X	X	9-1-1 needs necessarily require physical or logical isolation of some systems, even in a legacy environment. End-state NG9-1-1 systems have a degree of logical

														separation built into the architecture.
3	Applications	Detect	3.1	Run Automated Vulnerability Scanning Tools	Utilize an up-to-date Security Content Automation Protocol (SCAP) compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		X	X		X	X	X	X	
3	Applications	Detect	3.2	Perform Authenticated Vulnerability Scanning	Perform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested.		X	X		X	X		X	
3	Users	Protect	3.3	Protect Dedicated Assessment Accounts	Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.		X	X		X	X		X	
3	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.	X	X	X	X	X	X	X	X	
3	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.	X	X	X	X	X	X	X	X	
3	Applications	Respond	3.6	Compare Back-to-Back Vulnerability Scans	Regularly compare the results from consecutive vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.		X	X					x	

3	Applications	Respond	3.7	Utilize a Risk-Rating Process	Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities.		X	x					X	
4	Users	Detect	4.1	Maintain Inventory of Administrative Accounts	Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.		X	X		X	X	X	X	
4	Users	Protect	4.2	Change Default Passwords	Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.	X	X	X	X	X	X	X	X	
4	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.	X	X	X			X	X	X	
4	Users	Protect	4.4	Use Unique Passwords	Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		X	X		X	X	X	X	
4	Users	Protect	4.5	Use Multi-Factor Authentication for All Administrative Access	Use multi-factor authentication and encrypted channels for all administrative account access.		X	X	X	X	X	X	X	NG9-1-1 standards require MFA for identify providers and otherwise strongly encourage that all accounts are protected by MFA.
4	Users	Protect	4.6	Use Dedicated Workstations For All Administrative Tasks	Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading			X			X	X	X	NG9-1-1 provides for a trust framework that allows an elevated level of privilege for all trusted members of the NG9-1-1 community. Accordingly, this requirement should

					e-mail, composing documents, or browsing the Internet.									apply all the way through the ecosystem.
4	Users	Protect	4.7	Limit Access to Script Tools	Limit access to scripting tools (such as Microsoft® PowerShell and Python) to only administrative or development users with the need to access those capabilities.		X	X		X	X		X	
4	Users	Detect	4.8	Log and Alert on Changes to Administrative Group Membership	Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.		X	X		X	X		X	
4	Users	Detect	4.9	Log and Alert on Unsuccessful Administrative Account Login	Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.		X	X		X	X		X	
5	Applications	Protect	5.1	Establish Secure Configurations	Maintain documented security configuration standards for all authorized operating systems and software.	X	X	X	X	X	X	X	X	
5	Applications	Protect	5.2	Maintain Secure Images	Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.		X	X		X	X		X	
5	Applications	Protect	5.3	Securely Store Master Images	Store the master images and templates on securely configured servers, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible.		X	X		X	X		X	
5	Applications	Protect	5.4	Deploy System Configuration Management Tools	Deploy system configuration management tools that will automatically enforce and redeploy		X	X		X	X		X	

					configuration settings to systems at regularly scheduled intervals.									
5	Applications	Detect	5.5	Implement Automated Configuration Monitoring Systems	Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.		X	X		X	X		X	
6	Network	Detect	6.1	Utilize Three Synchronized Time Sources	Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.		X	X		X	X	X	X	GPS clocks and authoritative time are well-established concepts even in legacy 9-1-1, where log records are auditable and timestamps used as evidence in legal proceedings.
6	Network	Detect	6.2	Activate Audit Logging	Ensure that local logging has been enabled on all systems and networking devices.	X	X	X	X	X	X	X	X	Logging is a long-established concept in 9-1-1; calls and dispatch events have long been logged and timestamped for legal purposes.
6	Network	Detect	6.3	Enable Detailed Logging	Enable system logging to include detailed information such as a event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		X	X	X	X	X	X	X	Logging is a long-established concept in 9-1-1; calls and dispatch events have long been logged and timestamped for legal purposes.
6	Network	Detect	6.4	Ensure Adequate Storage for Logs	Ensure that all systems that store logs have adequate storage space for the logs generated.		X	X	X	X	X	X	X	
6	Network	Detect	6.5	Central Log Management	Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.		X	X		X	X	X	X	NG9-1-1 provides for a permissions-based interoperable logging service that is used more or less in-realtime in communications during an incident. However,

														there is no reasonable expectation the legacy or transitional NG9-1-1 networks support this service. Security and interoperability are managed through a standardized trust framework.
6	Network	Detect	6.6	Deploy SIEM or Log Analytic Tools	Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.		X	X		X	X		X	
6	Network	Detect	6.7	Regularly Review Logs	On a regular basis, review logs to identify anomalies or abnormal events.		X	X		X	X		X	
6	Network	Detect	6.8	Regularly Tune SIEM	On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.			X			X		X	
7	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.	X	X	X	X	X	X	X	X	
7	Applications	Protect	7.2	Disable Unnecessary or Unauthorized Browser or Email Client Plugins	Uninstall or disable any unauthorized browser or email client plugins or add-on applications.		X	X		X	X		X	
7	Applications	Protect	7.3	Limit Use of Scripting Languages in Web Browsers and Email Clients	Ensure that only authorized scripting languages are able to run in all web browsers and email clients.		X	X		X	X		X	
7	Network	Protect	7.4	Maintain and Enforce Network-Based URL Filters	Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they		X	X		X	X		X	

					are physically at an organization's facilities or not.									
7	Network	Protect	7.5	Subscribe to URL-Categorization Service	Subscribe to URL-categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default.		X	X		X	X		X	
7	Network	Detect	7.6	Log All URL requester	Log all URL requests from each of the organization's systems, whether on-site or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.		X	X		X	X		X	
7	Network	Protect	7.7	Use of DNS Filtering Services	Use Domain Name System (DNS) filtering services to help block access to known malicious domains.	X	X	X	X	X	X	X	X	
7	Network	Protect	7.8	Implement DMARC and Enable Receiver-Side Verification	To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail(DKIM) standards.		X	X		X	X		X	
7	Network	Protect	7.9	Block Unnecessary File Types	Block all email attachments entering the organization's email gateway if the file types are unnecessary for the organization's business.		X	X		X	X		X	
7	Network	Protect	7.10	Sandbox All Email Attachments	Use sandboxing to analyze and block inbound email attachments with malicious behavior.			X			X		X	
8	Devices	Protect	8.1	Utilize Centrally Managed Anti-malware Software	Utilize centrally managed anti-malware software to continuously monitor and defend each of the		X	X		X	X		X	

					organization's workstations and servers.									
8	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.	X	X	X	X	X	X	X	X	
8	Devices	Protect	8.3	Enable Operating System Anti-Exploitation Features/Deploy Anti-Exploit Technologies	Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		X	X		X	X		X	
8	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.	X	X	X	X	X	X	X	X	
8	Devices	Protect	8.5	Configure Devices to Not Auto-Run Content	Configure devices to not auto-run content from removable media.	X	X	X	X	X	X	X	X	
8	Devices	Detect	8.6	Centralize Anti-Malware Logging	Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting.		X	X		X	X		X	
8	Network	Detect	8.7	Enable DNS Query Logging	Enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains.		X	X		X	X		X	
8	Devices	Detect	8.8	Enable Command-Line Audit Logging	Enable command-line audit logging for command shells, such as Microsoft PowerShell and Bash.		X	X		X	X		X	
9	Devices	Identify	9.1	Associate Active Ports, Services, and Protocols to Asset Inventory	Associate active ports, services, and protocols to the hardware assets in the asset inventory.		X	X		X	X		X	
9	Devices	Protect	9.2	Ensure Only Approved Ports, Protocols, and Services Are Running	Ensure that only network ports, protocols, and services listening on a system with validated business needs are running on each system.		X	X		X	X		X	

9	Devices	Detect	9.3	Perform Regular Automated Port Scans	Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.		X	X		X	X		X	
9	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.	X	X	X	X	X	X	X	X	Though standalone firewalls are diminishing in practical utility in a modern world, it is common practice to implement firewall functionality at the ingress and egress of ESInets, including transitional ESInets.
9	Devices	Protect	9.5	Implement Application Firewalls	Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged.			X		X	X	X	X	Though standalone firewalls are diminishing in practical utility in a modern world, it is common practice to implement firewall functionality at the ingress and egress of ESInets, including transitional ESInets.
10	Data	Protect	10.1	Ensure Regular Automated BackUps	Ensure that all system data is automatically backed up on a regular basis.	X	X	X	X	X	X	X	X	
10	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.	X	X	X	X	X		X	X	
10	Data	Protect	10.3	Test Data on Backup Media	Test data integrity on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.		X	X		X	X	X	X	

10	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.	X	X	X	X	X	X	X	X	
10	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.	X	X	X	X	X	X	X	X	
11	Network	Identify	11.1	Maintain Standard Security Configurations for Network Devices	Maintain documented security configuration standards for all authorized network devices.		X	X		X	X	X	X	NG9-1-1 requires a certain level of documentation to pass validation and be allowed as a member of the trust chain at all, so it is reasonable to expect that all participating parties (including ECCs) maintain this documentation.
11	Network	Identify	11.2	Document Traffic Configuration Rules	All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.		X	X		X	X			
11	Network	Detect	11.3	Use Automated Tools to Verify Standard Device Configurations and Detect Changes	Compare all network device configuration against approved security configurations defined for each network device in use, and alert when any deviations are discovered.		X	X		X	X	X	X	
11	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.	X	X	X		X	X	X	X	

11	Network	Protect	11.5	Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions	Manage all network devices using multi-factor authentication and encrypted sessions.		X	X		X	X	X	X	In end-state NG9-1-1, all communications are protected by TLS.
11	Network	Protect	11.6	Use Dedicated Machines For All Network Administrative Tasks	Ensure network engineers use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be segmented from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading email, composing documents, or surfing the Internet.		X	X		X	X		X	
11	Network	Protect	11.7	Manage Network Infrastructure Through a Dedicated Network	Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.		X	X		X	X	X	X	
12	Network	Identify	12.1	Maintain an Inventory of Network Boundaries	Maintain an up-to-date inventory of all of the organization's network boundaries.	X	X	X	X	X	X	X	X	
12	Network	Detect	12.2	Scan for Unauthorized Connections Across Trusted Network Boundaries	Perform regular scans from outside each trusted network boundary to detect any unauthorized connections which are accessible across the boundary.		X	X		X	X	X	X	
12	Network	Protect	12.3	Deny Communications With Known Malicious IP Addresses	Deny communications with known malicious or unused Internet IP addresses and limit access only to trusted and necessary IP address ranges at each of the organization's network boundaries.		X	X		X	X	X	X	NG9-1-1 creates a trusted environment, so most transactions are assumed to be malicious unless proven to be trustworthy ahead of time.

12	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.	X	X	X	X	X	X	X	X	
12	Network	Detect	12.5	Configure Monitoring Systems to Record Network Packets	Configure monitoring systems to record network packets passing through the boundary at each of the organization's network boundaries.		X	X		X	X	X	X	
12	Network	Detect	12.6	Deploy Network-Based IDS Sensors	Deploy network-based Intrusion Detection Systems (IDS) sensors to look for unusual attack mechanisms and detect compromise of these systems at each of the organization's network boundaries.		X	X		X	X		X	
12	Network	Protect	12.7	Deploy Network-Based Intrusion Prevention Systems	Deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the organization's network boundaries.			X			X	X	X	
12	Network	Detect	12.8	Deploy NetFlow Collection on Networking Boundary Devices	Enable the collection of NetFlow and logging data on all network boundary devices.		X	X		X	X		X	
12	Network	Detect	12.9	Deploy Application Layer Filtering Proxy Server	Ensure that all network traffic to or from the Internet passes through an authenticated application layer proxy that is configured to filter unauthorized connections.			X			X	X	X	
12	Network	Detect	12.10	Decrypt Network Traffic at Proxy	Decrypt all encrypted network traffic at the boundary proxy prior to analyzing the content. However, the organization may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic.			X	N/A	N/A	N/A	N/A	N/A	For the safety and security of callers and jurisdictions, NG9-1-1 traffic must not be decrypted in transit.

12	Users	Protect	12.11	Require All Remote Login to Use Multi-Factor Authentication	Require all remote login access to the organization's network to encrypt data in transit and use multi-factor authentication.		X	X		X	X	X	X
12	Devices	Protect	12.12	Manage All Devices Remotely Logging into Internal Network	Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.			X			X	X	X
13	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.	X	X	X	X	X	X	X	X
13	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.	X	X	X	X	X	X	X	X
13	Data	Detect	13.3	Monitor and Block Unauthorized Network Traffic	Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.			X			X	X	X
13	Data	Protect	13.4	Only Allow Access to Authorized Cloud Storage or Email Providers	Only allow access to authorized cloud storage or email providers.		X	X		X	X	X	X
13	Data	Detect	13.5	Monitor and Detect Any Unauthorized Use of Encryption	Monitor all traffic leaving the organization and detect any unauthorized use of encryption.			X			X	X	X

13	Data	Protect	13.6	Encrypt Mobile Device Data	Utilize approved cryptographic mechanisms to protect enterprise data stored on all mobile devices.	X	X	X	X	X	X	X	X	
13	Data	Protect	13.7	Manage USB Devices	If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.		X	X		X	X	X	X	
13	Data	Protect	13.8	Manage System's External Removable Media's Read/Write Configurations	Configure systems not to write data to external removable media, if there is no business need for supporting such devices.			X			X	X	X	
13	Data	Protect	13.9	Encrypt Data on USB Storage Devices	If USB storage devices are required, all data stored on such devices must be encrypted while at rest.			X			X	X	X	
14	Network	Protect	14.1	Segment the Network Based on Sensitivity	Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).		X	X		X	X	X	X	
14	Network	Protect	14.2	Enable Firewall Filtering Between VLANs	Enable firewall filtering between VLANs to ensure that only authorized systems are able to communicate with other systems necessary to fulfill their specific responsibilities.		X	X		X	X	X	X	
14	Network	Protect	14.3	Disable Workstation to Workstation Communication	Disable all workstation-to-workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems, through technologies such as Private VLANs or micro segmentation.		X	X		X				While a feasible and reasonable expectation for normal IT systems, including transitional ESInets that do nut use all of NG9-1-1's features, NG9-1-1 systems require interoperability between agents that constitutes lateral communication within and across the organization. NG9-1-1

														provides for special security controls to accommodate this.
14	Data	Protect	14.4	Encrypt All Sensitive Information in Transit	Encrypt all sensitive information in transit.		X	X		X	X	X	X	
14	Data	Detect	14.5	Utilize an Active Discovery Tool to Identify Sensitive Data	Utilize an active discovery tool to identify all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located on-site or at a remote service provider, and update the organization's sensitive information inventory.			X			X	X	X	
14	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.	X	X	X	X	X	X	X	X	
14	Data	Protect	14.7	Enforce Access Control to Data Through Automated Tools	Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system.			X				X	X	
14	Data	Protect	14.8	Encrypt Sensitive Information at Rest	Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			X				X	X	
14	Data	Detect	14.9	Enforce Detail Logging for Access or Changes to Sensitive Data	Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such			X				X	X	

					as File Integrity Monitoring or Security Information and Event Monitoring).									
15	Network	Identify	15.1	Maintain an Inventory of Authorized Wireless Access Points	Maintain an inventory of authorized wireless access points connected to the wired network.		X	X		X	X			
15	Network	Detect	15.2	Detect Wireless Access Points Connected to the Wired Network	Configure network vulnerability scanning tools to detect and alert on unauthorized wireless access points connected to the wired network.		X	X		X	X			
15	Network	Detect	15.3	Use a Wireless Intrusion Detection System	Use a wireless intrusion detection system (WIDS) to detect and alert on unauthorized wireless access points connected to the network.		X	X		X	X			
15	Devices	Protect	15.4	Disable Wireless Access on Devices if Not Required	Disable wireless access on devices that do not have a business purpose for wireless access.			X			X			
15	Devices	Protect	15.5	Limit Wireless Access on Client Devices	Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks.			X			X			
15	Devices	Protect	15.6	Disable Peer-to-Peer Wireless Network Capabilities on Wireless Clients	Disable peer-to-peer (ad hoc) wireless network capabilities on wireless clients.		X	X		X		N/A	N/A	While feasible and practical for business networks, some public safety functions, including MCPTT, require some support for peer-to-peer wireless communications between clients. These functions should work within a framework suitable for NG9-1-1's mission.

15	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.	X	X	X	X	X	X	x	x
15	Network	Protect	15.8	Use Wireless Authentication Protocols That Require Mutual, Multi-Factor Authentication	Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS), which requires mutual, multi-factor authentication.			X					x
15	Devices	Protect	15.9	Disable Wireless Peripheral Access of Devices	Disable wireless peripheral access of devices [such as Bluetooth and Near Field Communication (NFC)], unless such access is required for a business purpose.		X	X					x
15	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.	X	X	X	x	x	x	x	x
16	Users	Identify	16.1	Maintain an Inventory of Authentication Systems	Maintain an inventory of each of the organization's authentication systems, including those located on-site or at a remote service provider.		X	X		x	x	x	x
16	Users	Protect	16.2	Configure Centralized Point of Authentication	Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		X	X		x	x	x	x
16	Users	Protect	16.3	Require Multi-Factor Authentication	Require multi-factor authentication for all user accounts, on all systems, whether managed on-site or by a third-party provider.		X	X		X	X	X	X
16	Users	Protect	16.4	Encrypt or Hash all Authentication Credentials	Encrypt or hash with a salt all authentication credentials when stored.		X	X		X	X	X	X
16	Users	Protect	16.5	Encrypt Transmittal of Username and Authentication Credentials	Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.		X	X		X	X	X	X

16	Users	Identify	16.6	Maintain an Inventory of Accounts	Maintain an inventory of all accounts organized by authentication system.		X	X		X	X	X	X	
16	Users	Protect	16.7	Establish Process for Revoking Access	Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.		X	X		X	X		X	
16	Users	Respond	16.8	Disable Any Unassociated Accounts	Disable any account that cannot be associated with a business process or business owner.	X	X	X	X	X	X	X	X	
16	Users	Respond	16.9	Disable Dormant Accounts	Automatically disable dormant accounts after a set period of inactivity.	X	X	X	X	X	X	X	X	
16	Users	Protect	16.10	Ensure All Accounts Have An Expiration Date	Ensure that all accounts have an expiration date that is monitored and enforced.		X	X		X	X	X	X	
16	Users	Protect	16.11	Lock Workstation Sessions After Inactivity	Automatically lock workstation sessions after a standard period of inactivity.	X	X	X	X	X	X	X	X	
16	Users	Detect	16.12	Monitor Attempts to Access Deactivated Accounts	Monitor attempts to access deactivated accounts through audit logging.		X	X					X	
16	Users	Detect	16.13	Alert on Account Login Behavior Deviation	Alert when users deviate from normal login behavior, such as time-of-day, workstation location, and duration.			X					X	
17	N/A	N/A	17.1	Perform a Skills Gap Analysis	Perform a skills gap analysis to understand the skills and behaviors workforce members are not adhering to, using this information to build a baseline education roadmap.		X	X	X	X	X	X	X	CSRIC recommends that all organizations of all sizes and implementation phases perform a basic cybersecurity audit against these recommendations.
17	N/A	N/A	17.2	Deliver Training to Fill the Skills Gap	Deliver training to address the skills gap identified to positively impact workforce members' security behavior.		X	X	X	X	X	X	X	CSRIC recommends that all organizations of all sizes and implementation phases perform basic

														cybersecurity training against these recommendations.
17	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.	X	X	X	X	X	X	X	X	
17	N/A	N/A	17.4	Update Awareness Content Frequently	Ensure that the organization's security awareness program is updated frequently (at least annually) to address new technologies, threats, standards, and business requirements.		X	X	X	X	X	X	X	
17	N/A	N/A	17.5	Train Workforce on Secure Authentication	Train workforce members on the importance of enabling and utilizing secure authentication.	X	X	X	X	X	X	X	X	
17	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.	X	X	X	X	X	X	X	X	
17	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.	X	X	X	X	X	X	X	X	
17	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.	X	X	X	X	X	X	X	X	
17	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.	X	X	X	X	X	X	X	X	

18	N/A	N/A	18.1	Establish Secure Coding Practices	Establish secure coding practices appropriate to the programming language and development environment being used.		X	X		X	X	X	X	The 9-1-1 community does not develop a tremendous amount of software in-house; however, when procuring services, 9-1-1 entities should require their providers to document their adherence to these controls.
18	N/A	N/A	18.2	Ensure That Explicit Error Checking is Performed for All In-House Developed Software	For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.		X	X		X	X	X	X	
18	N/A	N/A	18.3	Verify That Acquired Software is Still Supported	Verify that the version of all software acquired from outside your organization is still supported by the developer or appropriately hardened based on developer security recommendations.		X	X		X	X	X	X	
18	N/A	N/A	18.4	Only Use Up-to-Date and Trusted Third-Party Components	Only use up-to-date and trusted third-party components for the software developed by the organization.			X		X	X	X	X	
18	N/A	N/A	18.5	Use Only Standardized and Extensively Reviewed Encryption Algorithms	Use only standardized, currently accepted, and extensively reviewed encryption algorithms.		X	X		X	X	X	X	
18	N/A	N/A	18.6	Ensure Software Development Personnel are Trained in Secure Coding	Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities.		X	X		X	X	X	X	
18	N/A	N/A	18.7	Apply Static and Dynamic Code Analysis Tools	Apply static and dynamic analysis tools to verify that secure coding practices are being adhered to for internally developed software.		X	X		X	X	X	X	

18	N/A	N/A	18.8	Establish a Process to Accept and Address Reports of Software Vulnerabilities	Establish a process to accept and address reports of software vulnerabilities, including providing a means for external entities to contact your security group.		X	X		X	X	X	X	
18	N/A	N/A	18.9	Separate Production and Non-Production Systems	Maintain separate environments for production and non-production systems. Developers should not have unmonitored access to production environments.		X	X		X	X	X	X	
18	N/A	N/A	18.10	Deploy Web Application Firewalls	Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed.		X	X		X	X	X	X	
18	N/A	N/A	18.11	Use Standard Hardening Configuration Templates for Databases	For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested.		X	X		X	X	X	X	
19	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.	X	X	X	X	X	X	X	X	
19	N/A	N/A	19.2	Assign Job Titles and Duties for Incident Response	Assign job titles and duties for handling computer and network incidents to specific individuals, and ensure tracking and documentation		X	X		X	X		X	

					throughout the incident through resolution.									
19	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.	X	X	X	X	X	X	X	X	
19	N/A	N/A	19.4	Devise Organization-wide Standards for Reporting Incidents	Devise organization-wide standards for the time required for system administrators and other workforce members to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification.		X	X		X	X		X	
19	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.	X	X	X	X	X	X	X	X	
19	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.	X	X	X	X	X	X	X	X	
19	N/A	N/A	19.7	Conduct Periodic Incident Scenario Sessions for Personnel	Plan and conduct routine incident, response exercises and scenarios for the workforce involved in the incident response to maintain awareness and comfort in responding to real-world threats. Exercises should test communication channels, decision making, and incident responders technical capabilities using tools and data available to them.		X	X		X	X	X	X	

19	N/A	N/A	19.8	Create Incident Scoring and Prioritization Schema	Create incident scoring and prioritization schema based on known or potential impact to your organization. Utilize score to define frequency of status updates and escalation procedures.			X			X	X	X	
20	N/A	N/A	20.1	Establish a Penetration Testing Program	Establish a program for penetration tests that includes a full scope of blended attacks, such as wireless, client-based, and web application attacks.		X	X		X	X	X	X	In general, all members of the 9-1-1 community should exercise their systems, particularly in an end-state NG9-1-1 environment. While normally not a reasonable requirement for small businesses, even a small ECC must be required to demonstrate that they are reputable, trustworthy members of the overall disaggregated NG9-1-1 system.
20	N/A	N/A	20.2	Conduct Regular External and Internal Penetration Tests	Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully.		X	X		X	X	X	X	
20	N/A	N/A	20.3	Perform Periodic Red Team Exercises	Perform periodic Red Team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively.			X			X	X	X	
20	N/A	N/A	20.4	Include Tests for Presence of Unprotected System Information and Artifacts	Include tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, e-mails or documents containing passwords or other information critical to system operation.		X	X		X	X	X	X	

20	N/A	N/A	20.5	Create Test Bed for Elements Not Typically Tested in Production	Create a test bed that mimics a production environment for specific penetration tests and Red Team attacks against elements that are not typically tested in production, such as attacks against supervisory control and data acquisition and other control systems.		X	X		X	X	X	X
20	N/A	N/A	20.6	Use Vulnerability Scanning and Penetration Testing Tools in Concert	Use vulnerability scanning and penetration testing tools in concert. The results of vulnerability scanning assessments should be used as a starting point to guide and focus penetration testing efforts.		X	X		X	X	X	X
20	N/A	N/A	20.7	Ensure Results from Penetration Test are Documented Using Open, Machine-readable Standards	Wherever possible, ensure that Red Team results are documented using open, machine-readable standards (e.g., SCAP). Devise a scoring method for determining the results of Red Team exercises so that results can be compared over time.			x			X	X	X
20	N/A	N/A	20.8	Control and Monitor Accounts Associated with Penetration Testing	Any user or system accounts used to perform penetration testing should be controlled and monitored to make sure they are only being used for legitimate purposes, and are removed or restored to normal function after testing is over.		X	X		X	X	X	X

10 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."[107] Others reflect generally available descriptions found on the Internet.

Term	Description
ADR (Additional Data Repository)	A data storage facility for Additional Data. The ADR dereferences a request from the NGCS or PSAP to return additional information about the call, caller or location.
ALI (Automatic Location Identification)	The automatic display at the PSAP of the caller's telephone number, the address/location of the telephone and supplementary emergency services information of the location from which a call originates.
ALI (Automatic Location Identification)	The automatic display at the PSAP of the caller's telephone number, the address/location of the telephone and supplementary emergency services information of the location from which a call originates.
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.
CAD (Computer Aided Dispatch)	A computer-based system, which aids PSAP Telecommunicators by automating selected dispatching and record keeping activities.
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.
CRL (Certificate Revocation List)	A list of digital certificates that have been revoked by the issuing certificate authority (CA) before their scheduled expiration date and should no longer be trusted
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.

[107] "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**
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.
DANE (DNS-based Authentication of Named Entities)	An Internet security protocol to allow X.509 digital certificates, commonly used for Transport Layer Security (TLS), to be bound to domain names using Domain Name System Security Extensions (DNSSEC).
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.
DMZ (Demilitarized Zone)	In computer security, a DMZ Network [sometimes referred to as a "demilitarized zone"] functions as a subnetwork containing an organization's exposed, outward-facing services and it acts as the exposed point to untrusted networks, like the Internet)
DNS (Domain Name Service)	A globally distributed database for the resolution of host names to numeric IP addresses.
DPKI (Decentralized PKI)	Eliminates dependence on centralized registries for identifiers as well as centralized certificate authorities for key management, which is the standard in hierarchical PKI.
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.
ESRP (Emergency Services Routing Proxy)	An i3 functional element which is a SIP proxy server that selects the next hop routing within the ESInet based on location and policy. There is an ESRP on the edge of the ESInet. There is usually an ESRP at the entrance to an NG9-1-1 PSAP. There may be one or more intermediate ESRPs between them.

Term	Description
ESS (Emergency Services Sector)	A system of preparedness, response, and recovery elements that form the Nation's first line of defense for preventing and mitigating the risk from physical and cyber attacks, and manmade and natural disasters.
FICAM (Federal Government's implementation of Identity, Credential, and Access Management)	FICAM. It is meant to provide a common set of ICAM standards, best practices, and implementation guidance for Federal agencies.
GIS (Geographic Information System)	A system for capturing, storing, displaying, analyzing and managing data and associated attributes which are spatially referenced.
HTTPS (Hypertext Transfer Protocol Secure (HTTPS)	An extension of the Hypertext Transfer Protocol (HTTP). It is used for secure communication over a computer network, and is widely used on the Internet
ICAM (Identity Credentialing Access Management)	ICAM encompasses standardized core capabilities to be able to identify, authenticate, and authorize individuals and provides appropriate access to resources, which is the lynchpin to the success of the national cybersecurity initiative.
IDPS (Intrusion Detection and Preventions Systems)	Monitors network traffic for signs of a possible attack. When it detects potentially dangerous activity, it takes action to stop the attack
IDS (intrusion detection system)	A device, or software application that monitors a network or systems for malicious activity or policy violations.
MMS (Multi-media Message Service)	A standard way to send messages that extends the core SMS (Short Message Service) capability to include multimedia content to and from a mobile phone over a cellular network.
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.
NCCIC (National Cybersecurity and Communications Integration Center)	Acts to coordinate various aspects of the U.S. federal government's cybersecurity and cyberattack mitigation efforts, through cooperation with civilian agencies, infrastructure operators, state and local governments, and international partners.
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/
PBX (Private Branch Exchange)	Private Branch Exchange - a phone switch located at the customer's premise. (2020 Voip-info.org https://www.voip-info.org/pbx/)
PII (Personally Identifiable Information)	Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.
PKI (Public Key Infrastructure)	A set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.

Term	**Description**
PKIX (Public Key Infrastructure for X.509)	An ITU-T standard for a public key infrastructure (PKI) and Privilege Management Infrastructure (PMI). In NG9-1-1, refers to the format of a certificate containing a public key.
PPTP (Point-to-Point Tunneling Protocol)	An obsolete method for implementing virtual private networks.
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.
RDP (Remote Desktop Protocol)	Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft which provides a user with a graphical interface to connect to another computer over a network connection.
RMS (Records Management Systems)	The management of records for an organization throughout the records-life cycle. The activities in this management include the systematic and efficient control of the creation, maintenance, and destruction of the records along with the business t55ransactions associated with them. Considered a key component of operational efficiency, record management adds more value to organization’s information assets. https://www.techopedia.com/definition/30667/records-management-system-rms
SEM (security event management)	In general, SEM is concerned with real-time monitoring of logs and correlation of events
SIEM (security information and event management)	SIEM combines SIM (security information management) and SEM (security event management) functions into one security management system.
SIM (security information management)	A type of software that automates the collection of event log data from security devices, such as such as firewalls, proxy servers, intrusion-detection systems and antivirus software.
SIP (Session Initiation Protocol)	A protocol specified by the IETF (RFC3261) that defines a method for establishing multimedia sessions. Used as the call signaling protocol in Voice over IP, NENA i2, NENA i3 and IP Multimedia Subsystem.
SLTT (State, Local, Tribal And Territorial)	A term referring to four categories of governmental entities.
SMB (Server Message Block)	A network file sharing protocol that allows applications on a computer to read and write to files and to request services from server programs in a computer network.
SMS (Short Message Service)	A store-and-forward service typically provided by mobile carriers that sends short (160 characters or fewer) complete messages to an endpoint.
SSL (Secure Socket layer)	A computer networking protocol that manages server authentication, client authentication and encrypted communication between servers and clients.
SWIM (System Wide Information Management	The SWIM Program is a National Airspace System (NAS)-wide information system that supports Next Generation Air Transportation System (NextGen) goals.
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)

Term	Description
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.
TLS (Transport Layer Security)	An Internet protocol that operates between the IP layer and TCP and provides hop-by-hop authentication, integrity protection and privacy using a negotiated cipher-suite.
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)
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/
VPN (virtual private network)	A network implemented on top of another network, and private from it, providing transparent services between networks or devices and networks. VPNs often use some form of cryptographic security to provide this separation.