

Task Force on Optimal PSAP Architecture

An FCC Federal Advisory Committee



December 10th, 2015

WORKING GROUP 1

Optimal Cybersecurity Approach for PSAPs

Table of Contents

1	Introduction	4
1.1	Working Group 1 Team Members.....	6
2	Objective, Scope, and Methodology	7
2.1	Objective.....	7
2.2	Scope	7
2.3	Methodology.....	8
2.3.1	Use Case Methodology	8
3	Currently Used Security Practices.....	9
3.1	Current PSAP environment – Cybersecurity Today.....	9
3.1.1.1	Overarching Information Security Management System (ISMS).....	9
3.1.1.2	Documented Policies, Procedures and Controls in support of the ISMS.....	9
3.1.1.3	Compliance.....	9
3.1.1.4	Awareness	10
3.1.2	Access Control	10
3.1.2.1	Policy identifies proper approval based on access gates and ratings	10
3.1.2.2	Physical Security – Limited access and based on need to know.....	10
3.1.2.3	Human Resources.....	10
3.1.3	Security Controls	10
3.1.3.1	Business Continuity Plan/Disaster Recovery (BCP/DR).....	10
3.1.3.2	Geo-diverse in Active/Active or N+1 computing element configurations	11
3.1.3.3	Media Handling.....	11
3.1.3.4	Incident Management.....	11
3.1.3.5	Testing.....	11
3.1.3.6	Vulnerability Management.....	11
3.1.4	Internal network security and monitoring.....	11
3.1.4.1	Internal network security, Private DNS (internal facing only)	11
3.1.4.2	External network connections	12
3.1.5	Network entry point security	12
3.2	Transitional NG9-1-1 Architectures.....	12
3.3	IMS and ESInets.....	14
4	Recommended Best Practices for Cybersecurity in both Transitional and Fully Deployed NG9-1-1 Systems.....	16
4.1	NIST Cybersecurity Framework (NCF).....	16
4.2	Security Considerations for Apps interfacing to/with public safety.....	19
4.3	Identity Credentialing Access Management (ICAM).....	19
4.3.1	ICAM Goals and Objectives	19
4.3.2	ICAM Intersection	19
4.3.3	FICAM Roadmap and Implementation Guidance	21
4.3.4	Value Proposition.....	22
4.3.5	Identity Management	22
4.3.6	Credential Management.....	23
4.3.7	Access Management	23

5	NICE Workforce Framework.....	23
5.1	DHS recommendations and resources.....	29
5.1.1	Technical Programs	29
5.1.2	Technical Solutions.....	30
5.2	CSRIC Best Practices Related to Public Safety	31
6	Proposed Approaches to NG9-1-1 Cybersecurity Architecture.....	32
6.1	The Emergency Communications Cybersecurity Center (EC3).....	32
6.2	Description of Intrusion Detection and Prevention Systems.....	32
6.3	Proposed Approach for IDPS in the NG9-1-1 Environment.....	34
6.3.1	The EC3 Concept Explained.....	38
6.3.2	Cost Considerations	40
6.3.2.1	Operational Costs and Considerations	40
6.3.2.2	Capital Costs and Considerations.....	41
6.3.2.3	Summary of Cost Considerations.....	41
7	Recommendations	42
8	Summary	45
	Appendix 1 – PSAP Cybersecurity Use Cases	47
	Appendix 2 – PSAP Cybersecurity Checklists and Roadmap to secure PSAPs and NG9-1-1 system	56
	Appendix 3 – PSAP Cybersecurity Resources	75

1 Introduction

As Public Safety Answering Point (PSAP) 9-1-1 networks transition from TDM-based to IP-based architecture, as part of the migration to Next Generation 9-1-1 (NG9-1-1), they will face increasing exposure to cyber threats and vulnerabilities that did not exist in the legacy 9-1-1 environment. Cyber risk management strategies are being developed for the communications sector that will benefit the NG9-1-1 ecosystem as a whole. Much of the proposed cybersecurity strategy in this document is based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework (NCF); National Initiative for Cybersecurity Education (NICE) framework for cybersecurity education; the ongoing work of the Communications Security, Reliability, and Interoperability Council (CSRIC); and current work either recently completed or underway from other authorities including the U.S. Department of Homeland Security (DHS), the Association of Public Safety Communications Officials (APCO), and the National Emergency Number Association (NENA).

To date, however, the overall approach to NG9-1-1 network security has been lacking in clear direction or architectural definitions. 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. Working Group 1 (WG1) was tasked with addressing these cybersecurity issues for today’s PSAPs and developing recommendations for PSAP-specific cybersecurity practices based on experience and the sources referenced above. WG1 was also challenged to examine these same cybersecurity issue for tomorrow’s PSAPs, in the context of NG9-1-1 systems and services.

This report includes several sections, each intended to impart specific information and recommendations to the public safety community at large and to the Commission. The report first addresses the methodologies used, then discusses current and emerging 9-1-1 ecosystems and how cybersecurity is addressed in the present environment. The discussion then examines the various resources available to shape the transition and eventual full conversion to Next Generation 9-1-1 cybersecurity programs and architectures. Again, many of the themes underlying these discussions, and this report, are drawn from work completed or underway by NIST, NICE, CSRIC, DHS, APCO, NENA, and other relevant authorities. Next, WG1 proposes a cooperative and synergistic approach to cybersecurity for emergency communications, including core cybersecurity services; interconnected monitoring and mitigation; and near real-time information sharing amongst multiple levels of public safety agencies and entities. WG1 also includes examples of alternative models, partnerships to be considered, and high-level pricing estimates. The intent of this approach is to provide recommendations for further study and to define core cybersecurity services that relate directly to the public safety and emergency communications enterprise, including both current legacy and future NG9-1-1 systems.

Finally, WG1 provides a set of recommendations to public safety leadership. These recommendations will identify options for local leaders to make informed decisions as to how to best integrate these services, programs, and partnerships from the PSAP, and broader 9-1-1 and emergency communications community, at the local operations level through state and regional partners and up to potential federal level resources.

When reviewing these recommendations, readers should recognize that not every PSAP will have the same needs, capabilities, or requirements, from either a personnel or network perspective. With this in mind, it is important to note that there are a number of deployment

options available to PSAPs at a local operations level, as well as a number of options for cooperative sharing of core cybersecurity infrastructure and capabilities. It is neither reasonable, nor expected, that each PSAP nationwide would be able to implement every core cybersecurity service, hire cybersecurity experts, and/or provide their own in-house version of those suggested core services. Instead, as with NG9-1-1 architecture options to be discussed in the WG2 report, cybersecurity core services, training and capabilities will likely be a combination of the most economic, technologically sound, and operationally effective technologies available. It is the intent of WG1 to provide options and information so that PSAPs, local agencies and 9-1-1 Authorities can make intelligent choices, from the available options, based on their local needs and capabilities.

In addition to the core report, WG1 has created three (3) appendices. The first is a set of use cases that are pertinent to PSAPs not only in an NG environment but in many cases even in today's PSAP system. The intent of these use cases is to make apparent just how vulnerable the PSAP, and emergency communications community, are to cybersecurity. The second appendix is a checklist for PSAPs to perform an honest, and thorough, self-assessment of their current cyber capabilities, gaps, and a proposed "roadmap" for PSAPs to correct identified gaps. The third appendix includes a set of resources for PSAPs with regard to cybersecurity. It is the hope, and intent, of this working group that the following work product will be of use to PSAPs around the Nation and to all emergency communications partners.

1.1 Working Group 1 Team Members

Name	Organization/Company
Tim May (Federal Project Officer)	Federal Communications Commission
Dana Zelman (FCC Liaison)	Federal Communications Commission
Steve Souder (TFOPA Committee Chair)	Fairfax County, VA
Dana Wahlberg (TFOPA Committee Vice- Chair)	Minnesota Department of Public Safety
Jay English (WG 1 Chair)	Association of Public Safety Communications Officials
David Holl (WG 2 Chair)	PA Emergency Management Agency
Commissioner Philip Jones (WG 3 Chair)	WA State Public Utility Commission
Mary Boyd	Intrado
Drew Morin	TeleCommunication Systems
April Heinze	Michigan Communications Directors Association
Robert Brown	National Public Safety Telecommunications Council
Anthony Montani	Verizon
Jeanna Green	Sprint
Heath McGinnis	Verizon
Dusty Rhoads	Department of Homeland Security
William Boyken	AT&T
Tony Metke	Motorola
Brad Blanken	Competitive Carriers Association
Bernard Aboba	Microsoft
Mehrdad Negahban	beamSmart
Michael Kennedy	Office of Director of National Intelligence
Mario Derango	Motorola
Traci Knight	Department of Homeland Security
Marc Linsner	Cisco
Richard Ray	National Association for the Deaf
Rebecca Ladew	Speech Communications Assistance by Telephone, Inc

Table 1 - List of Working Group Members

2 Objective, Scope, and Methodology

2.1 Objective

The objective of Working Group 1 is to address the issues of increasing exposure to cyber threats and vulnerabilities that did not exist in the legacy 9-1-1 environment, and develop recommendations for PSAP-specific Cybersecurity practices based on the NIST Cybersecurity Framework and other foundational resources that include the results of Federal cybersecurity focused reports and activities of CSRIC and DHS; industry specific standards bodies such as NENA, APCO, and ATIS; and commercial industry best practices.

As part of the objectives for this Working Group we will provide Public Safety specific cybersecurity recommendations to the FCC, and a “toolkit” for use in the PSAP community. This toolkit will allow the Commission to provide not only guidance, but useful examples of the impacts of Cybersecurity risks that can be placed on PSAPs. The toolkit will include:

- A realistic self-assessment guide for PSAPs to evaluate their current cybersecurity capabilities and risks;
- A roadmap for the creation and implementation of a successful Cybersecurity strategy that applies to local public safety levels of government, up to including State level government; and
- A list of potential resources for PSAPs and 9-1-1 Authorities to provide additional research and fact-finding sources.

2.2 Scope

The scope of this work is limited to the identification of cybersecurity issues and documentation of recommended cybersecurity practices for Public Safety Answering Points. In the context of this work effort, a local PSAP is much more than a stand-alone entity but rather is the connection point in a complex system of integrated networks that form the critical infrastructure necessary to enable delivery of life saving services. As a necessity, there must be reference to other network elements outside of the local PSAP construct. Given the scope of Next Generation communications networks and systems as a whole, it is impossible to delve into cybersecurity considerations for PSAPs without taking into account the existing capabilities of the eco-system of various commercial providers who interact with public safety. These include, but are not limited to the providers of 9-1-1 Customer Premise Equipment (CPE), Computer Aided Dispatch (CAD), Records Management Systems (RMS), Radio/Dispatch Console, Mobile Data, Telecommunications Networks, public safety database infrastructure, and interconnect services at both the voice and data levels.

As a result of these interdependencies, and based in no small part on the work already accomplished and published by the National Institute of Standards and Technology (NIST), the recent CSRIC IV working groups, and the Department of Homeland Security (DHS), this working group is to incorporate the work of these outside agencies and organizations into the proposed recommendations to the Commission. In addition, the working group is to keep the scope of the research and recommendations limited to the PSAP community. Identification of potential threats along with available mitigation strategies will be discussed. However, many of the elements needing to be protected will be outside of the direct control of the PSAP for many cyber threats. As a result, part of the scope of this work will also be to recognize and/or identify when an attack has occurred and these recognition steps will be included as part of the “toolkit”.

Not only the physical elements of cybersecurity will be researched and addressed. As noted in much of the work already done by NIST and DHS, the human factor is vital when preparing for and defending against cyber threats. As part of the scope of this work, the team will explore a number of issues related to personnel security including cyber hygiene, training, and other mitigation steps related directly to the personnel involved with day to day operations and maintenance of any public safety system.

2.3 Methodology

The reduction of any cybersecurity framework to practice is rooted in the ability to identify assets, owners of these assets, threats/risks to these assets, and methods to mitigate the threats/risks. The current architecture of the PSAP as defined by the Legacy and Next Generation PSAP checklists will serve as a starting point to understand the current PSAP ecosystem. The architecture under development by Working Group 2 will also be referenced as WG1 works to ensure “future proof” guidance recommendations for best practices.

Use cases will be used to communicate the types of cybersecurity threats to PSAPs as an illustrative tool for demonstrated vulnerabilities or attack surfaces currently threatening PSAPs today. Additional Use cases specific to the transitional network and the end state NG9-1-1 network will also be identified. Finally, some forward looking issues will be used to expand the context of the threat to the PSAP as a result of the expansion of the public safety ecosystem. The public safety ecosystem will include additional information sources and new “players” such as FirstNet, healthcare providers, insurance companies, and other entities that reflect the future emergence of the Internet of Things.

Based on review of cybersecurity frameworks and best practices from multiple sources including NIST, DHS, CSRIC, etc., the Working Group will develop a set of recommended PSAP specific cybersecurity practices. These recommendations will identify resources and tools for development of a PSAP specific cybersecurity strategy. The Working Group will also leverage the NICE Workforce Framework to provide guidance for PSAP cybersecurity workforce development and training plans.

2.3.1 Use Case Methodology

WG1 created four (4) public safety use cases to illustrate the importance, and immediate need, of addressing cybersecurity in the PSAP and in 9-1-1 networks and systems. In creating these use cases, the working group seeks to illustrate both existing threats and potential future threats. The use cases presented in this report are not specific to any PSAP configuration and they do not illustrate the numerous threat vectors that are present. In the interest of preserving operational security no specific PSAP elements, operations, or architectures are referenced.

The intent of presenting these use cases is to make it abundantly clear to the 9-1-1 community, and public safety in general, that cybersecurity is a very real concern. By demonstrating high level vulnerabilities and risks, it is the hope of the working group that these use cases will provide public safety entities with better situational awareness, create a focus on cybersecurity, and encourage immediate action on the part of 9-1-1 authorities, PSAPs and public safety entities in both educating their personnel and protecting their networks and systems.

3 Currently Used Security Practices

The movement to NG9-1-1 implies a progression from legacy architecture to the future vision. However, several elements of the future vision are not practical or available in today's business environment, thereby, giving way to transitional architectures that step toward NG9-1-1.

As detailed in the WG2 report, 9-1-1 solution architectures can be considered as a progression from the legacy state to the future vision state with transitional steps in between:

- Legacy 9-1-1 Architecture
- Transitional 9-1-1 Architectures
- NG9-1-1 - NENA i3, i3 "like"9-1-1 and IMS Architectures

While WG2 will delve into architectural options, the WG1 report will not consider each option individually. Instead, this report will address cybersecurity from an enterprise point of view. PSAPs, 9-1-1 authorities and local agencies will then have information from WG2 as to architecture options, and information from WG1 as to ways to defend their architecture choice regardless of what that specific choice is.

WG1 will begin the discussion of cybersecurity options by describing current cybersecurity practices in use today. PSAPs, 9-1-1 Authorities and agencies at all levels should consider a review, and implementation, of these practices immediately as they apply to current networks and systems.

3.1 *Current PSAP environment – Cybersecurity Today*

In this section, WG1 provides information on the current cybersecurity practices taken to protect Legacy and in some cases transitional PSAPs by existing commercial providers. Additionally, the NCF, the NICE Workforce Framework, and the work of CSRIC Working Group 2A¹ provide insight into relevant security issues and are critical to current as well as future operations. These documents are discussed in detail later in this report.

3.1.1.1 Overarching Information Security Management System (ISMS)

The ISMS is a set of policies concerned with information security management or information technology related risks. The governing principle of the ISMS is that an organization should design, implement and maintain a coherent set of policies, processes and systems to manage risks to its information assets, thus ensuring acceptable levels of information security risk.²

3.1.1.2 Documented Policies, Procedures and Controls in support of the ISMS

Documentation of the policies, procedures, and controls of the ISMS are necessary to ensure completeness, facilitate training, and measure effectiveness. This documentation is subject to regular update and revision as an ISMS must adapt to changes in both organization (participants) and the external environment (systems/assets).

3.1.1.3 Compliance

A clear understanding of all applicable information security requirements is imperative

¹ [Cyber Security Best Practices, March 2011]

² See "[Security management system's usability key to easy adoption](#)". [sourcesecurity.com](#).

to ensuring compliance. Regular internal and/or external audits are conducted to measure compliance with all laws, regulations, customer requirements, and subscribed best practices.

3.1.1.4 Awareness

A training program is established to ensure that participants are educated on the ISMS and their roles and responsibilities in execution. Best practices dictate that ongoing education using refresher training should also be augmented with alerts, reminders and tips as part of an overall security awareness program.

3.1.2 Access Control

Regarding rights and permissions, NENA 04-503 states, “It is important to understand the difference between a right and permission:

- A right is a property that is assignable to a user or a group, which will either allow or deny them the ability to perform an action. A good example of this is the ability to install a printer on a computer; this is an allowable right that can be assigned.
- A permission, on the other hand, grants or denies access to an object or resource. This would allow a basic user to see only their files while allowing management to see all of the files.”³

3.1.2.1 Policy identifies proper approval based on access gates and ratings

The organization should maintain a simple, useable structure, which can be administered by the fewest number of personnel possible. They should grant rights only to those who need them. There should be classes of security levels (*e.g.* general use, network administrator, *etc.*) and these roles are assigned pertinent access control.

3.1.2.2 Physical Security – Limited access and based on need to know

The organization should establish an acceptable use and access policy. All equipment should be housed in secure environments that only allow key card access to authorized personnel. All entry and egress from secure facilities should be logged. Only those authorized should be allowed access to secure facilities and all visitors must be escorted. Remote access to systems should be controlled via the appropriate passwords and certificates.

3.1.2.3 Human Resources

Human Resource (HR) procedures should be developed to include preventative measures such as background checks. Procedures should acknowledge that job rotations may necessitate the need for modifying the access of the rotated personnel. The organization should have termination procedures that include returning of all keys, pass cards and sensitive material. The organization should have a code of conduct that outlines expectations of its personnel. Additional workplace policies may be required that are specific to the organization’s function.

3.1.3 Security Controls

What follows are specific methods for protecting information assets.

3.1.3.1 Business Continuity Plan/Disaster Recovery (BCP/DR)

The protection of information assets must include a detailed plan for business disruptions

³ See: http://c.ymcdn.com/sites/www.nena.org/resource/resmgr/Standards/NENA_04-503.1_Network_System.pdf

and instructions for recovery and resumption. This includes the identification of information security concerns in emergency situations.

3.1.3.2 Geo-diverse in Active/Active or N+1 computing element configurations

The availability of information needs to be addressed according to the criticality of the information. For mission critical information and services, geo-diverse sites should be considered. For non-essential information or services, a back-up of the information may be sufficient.

3.1.3.3 Media Handling

Controls for classification, labeling and treatment of all forms of media should be implemented. The organization should implement a removable media policy that restricts the use of or controls the use of removable media such as USB drives, external hard drives, *etc.* For transportation, media or devices containing sensitive information must be marked as such and hand delivered by the custodian. However, if there is an overriding business need to do otherwise then, with appropriate approval, it may be shipped in sealed packages utilizing recorded/certified delivery.

3.1.3.4 Incident Management

The ability to identify and respond quickly to an incident is essential to effective security. Incident management capability for security incidents includes preparation, detection and analysis, containment, eradication, and recovery.

3.1.3.5 Testing

Testing of configuration ensures that the security controls in place are effective. Testing can include penetration testing, application testing, BCP/DR tests, and control effectiveness.

3.1.3.6 Vulnerability Management

Regular scans for vulnerabilities should be run against the information system and hosted applications and when new vulnerabilities potentially affecting these system/applications are identified and reported. Hardening standards are used to ensure a secure configuration and enumerate improper configurations. The remediation of legitimate vulnerabilities identified should be prioritized according to the severity of the risk.

3.1.4 Internal network security and monitoring

Intrusion Detections Systems/Intrusion Prevention Systems are used to identify and/or prevent malware from getting to an organization's systems. External monitoring is the observation of events occurring at the information system boundary (*i.e.*, part of perimeter defense and boundary protection). Internal monitoring is the observation of events occurring within the information system.

3.1.4.1 Internal network security, Private DNS (internal facing only)

The information systems that collectively provide name and/or address resolution service for an organization implement internal/external role separation. This can ensure DNS servers with internal roles only process name and address resolution requests from within organizations (*i.e.*, from internal clients).

Network segregation can further reduce the attack surface of organizational information systems. Isolation of selected information system components is also a means of limiting the damage from successful cyber-attacks when those attacks occur. This Defense in Depth approach improves the ability of the defender to identify and mitigate an attack before it has a chance to impact overall operations.

3.1.4.2 External network connections

Network firewalls and Session Border Controllers should always be implemented whenever there is any access from external networks. Specific care should be taken if the access is from the Internet to prevent intrusion attacks such as Distributed Denial of Service (DDOS). Secure Virtual Private Networks (VPNs) are the current preferred method for providing external access into the systems. All computers that have external access (e.g. to the Internet) must incorporate the latest virus software. Section 5.1 of NENA's 08-003 identifies specific firewall and Session Border Control functions necessary to facilitate secure access.

3.1.5 Network entry point security

PSAP networks currently have multiple connection points from external, public networks. Specifically, the PSTN (including wireline, wireless and VoIP) and the Internet are used extensively to deliver information to and from PSAPs. These public network entry points are secured at the point of entry using various technologies and filters as described below:

1. SS7 messaging management/filtering (protects call control components) is implemented at the STP. The purpose is to ensure that only messages specifically required for emergency services implementation are allowed to pass.
2. IP data entry points (SIP for NextGen) use Border Control Functions (BCFs), including Session Border Controllers, Firewalls, packet filtering, message type limitations, encryption and secured authenticated external interfaces.
3. All ingress and egress paths are secured, communication occurs only between pre-authenticated entities. All ingress traffic to the system enters via a firewall or Session Border Controller. All connectivity is prearranged via a Network to Network Interface (NNI) agreement. Connectivity should be secured and encrypted via VPNs or IPSEC tunnels.
4. All communication of sensitive data is encrypted. Transport Layer Security (TLS) must be used for transmission between network elements to encrypt the message. In addition IPSEC may be used to manage internetwork connections.
5. Subnetworks for publicly accessible system components are implemented. The subnetworks are physically and/or logically separated from internal organizational networks.
6. The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception. Applicable to both inbound and outbound network communications traffic, a deny-all, permit-by-exception network communications traffic policy ensures that only those connections which are essential and approved are allowed.

3.2 Transitional NG9-1-1 Architectures

As previously noted, WG1 will not delve into specific architecture discussions.

However, in order to mirror the WG2 approach, we will note that in addition to the legacy 9-1-1 networks, and related cybersecurity practices, transitional NG9-1-1 architectures do exist, and will continue to be deployed and evolve. Several aspects of the NENA i3 architecture are barriers to immediate implementation. Primarily, OSPs are not prepared today to deliver 9-1-1 calls via IP technology with location information to 9-1-1 Service Providers. Transitional NG9-1-1 architectures have been defined that allow the movement to NG9-1-1 to begin. Two basic forms of transitional architectures exist:

- **IP Selective Router (IPSR):** An IPSR transition architecture replaces the legacy SR with an IP infrastructure and continues to process 9-1-1 calls based on the callers ANI and a mapped ESN. This approach allows the retirement of legacy selective routers with an IP infrastructure that is programmable and expandable to support the NENA i3 algorithms. The IPSR approach utilizes several of the “gateway elements”, or protocol conversion elements, also deployed in the NENA i3 transitional architecture.
- **NENA i3 Transitional Architecture:** For the purposes of this report, the transitional architecture will be treated in the same manner as a fully deployed NG9-1-1 network. Since the transitional architecture, which is fully discussed in the WG2 report, includes IP connectivity at some levels, and IP capabilities in the PSAP, it is important to defend this architecture in the same manner as any other IP network.

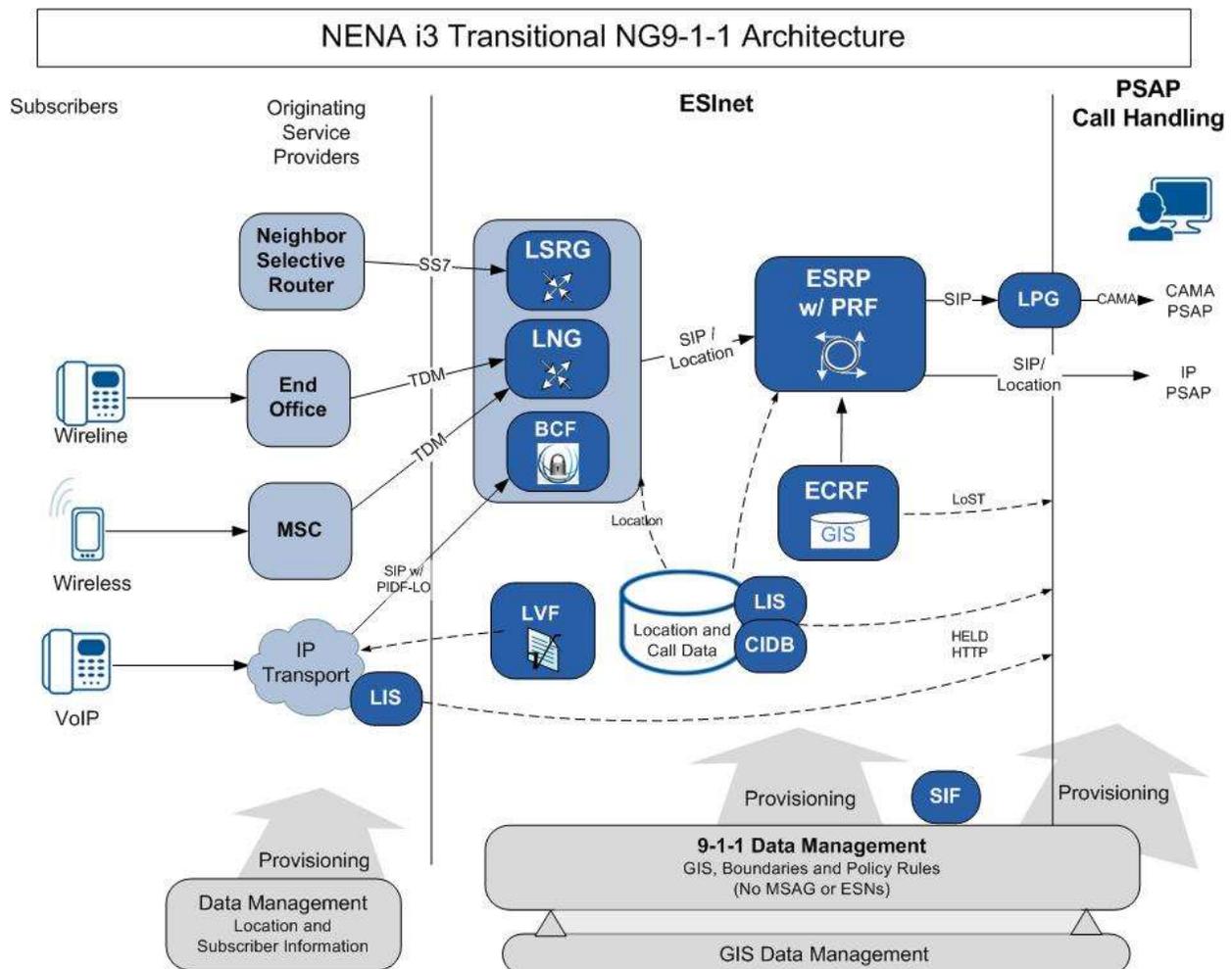


Figure 1 - NENA i3 Transitional NG9-1-1 Architecture

3.3 *IMS and ESInets*⁴

Portions of the content and the figure contained in this section have been reproduced from ATIS-0700015.v003 with permission from the Alliance for Telecommunications Industry Solutions (ATIS).

One of the major drivers in the advancement of communications technology as it relates to 9-1-1 is the deployment of IMS based networks and systems. Since the WG2 report does not address IMS as it relates to ESInets and NG9-1-1 systems, and since these networks will interface with both legacy and NG9-1-1 systems, they will need to be considered as part of the overall cybersecurity plan. Therefore, WG1 offers the following information with regard to IMS and ESInets.

“The purpose of the ATIS-0700015.v003 standard is to enable deployment in North America of support for Multimedia Emergency Services (MMES) calls in the IP domain from originating networks that conform to 3GPP IMS specifications. The standard is intended to complement the NENA i3 standard [Ref 100] and to define any changes and limitations to the 3GPP IMS solution that are needed for operation in North America.

The emergency services landscape within North America requires a greater level of detail than what has been specified in 3GPP. The ATIS document provides additional details to the 3GPP specifications with respect to emergency services for North America, specific to interconnection to both legacy emergency service networks and next generation emergency services networks.

North American IMS-based origination networks originate emergency calls (which include steps taken by the originating device and network elements) and route such calls to a NENA i3/NG9-1-1 ESInet (initial ingress ESInet) or legacy Selective Router. As part of call handling within the IMS origination network, the location (or an estimated location) of the originating device is determined and used to route the call to an appropriate ESInet entry point or to a legacy Selective Router. This location, or an updated and possibly more accurate version (via re-bid), can be made available to PSAPs for dispatch.

This standard identifies the types of media that can be delivered to each type of emergency services network, *i.e.*, legacy emergency services network and a NENA i3 ESInet. For example, voice, GTT, and session-mode text can be delivered to a legacy emergency services network via interworking. All types of media can be delivered to a NENA i3 ESInet.

This document describes IP emergency call support for IMS networks and includes North American-specific requirements, *e.g.*, on Reference Identifier assignment and location support, that in 3GPP documents are more generic. The document concentrates on common IMS-based origination networks supporting all classes of service; IMS aspects are mostly access-independent and not limited to mobile.

In the North American architecture, the emphasis is on the relationship between the originating IMS network and the interconnected emergency services network, rather than the

⁴ ATIS Standard for Implementation of 3GPP Common IMS Emergency Procedures for IMS Origination and ESInet/Legacy Selective Router Termination (ATIS-0700015.v003). © 2015 Alliance for Telecommunications Industry Solutions (ATIS). A copy may be obtained via <https://www.atis.org/docstore/product.aspx?id=28140>.

PSAP. For example, emergency calls destined for legacy PSAPs may be directed from the originating IMS network to a Selective Router in a legacy emergency services network or to an Emergency Services IP Network (ESInet) that hosts legacy PSAPs. Emergency calls destined for IP-capable PSAPs are directed from the originating IMS network to an ESInet. Thus, in North America, it is the capabilities of the interconnected emergency services network that influence call handling within the IMS originating network, rather than the specific capabilities of the PSAP to which the call will ultimately be delivered.

For calls to a NENA i3 ESInet, calls may be delivered with the location of the caller (location-by-value [LbyV]) or a location URI (location-by-reference [LbyR]) using a Reference Identifier that the ESInet may use to query the Common IMS Network for the location. The NENA i3 ESInet may query both during call set up and after the call has reached the PSAP.

If the Common IMS Network needs to acquire the location it may do so via a Location Server (LS). The characteristics of the LS may differ based upon the class of service. For example, for mobile calls, the Common IMS Network may query location determination equipment via the Location Server.

Once the Common IMS Network has location, it must select the appropriate emergency services network to deliver the call to. The LRF may use internal processes to access an integrated RDF to do this or it may interrogate an external RDF. Emergency calls may be delivered either to a NENA i3 ESInet, or to a legacy Selective Router.”⁵

Figure 2, extracted directly from the ATIS Standard, illustrates an expanded architecture that takes into account the network elements of NENA’s i3 architecture and legacy emergency services network. Except for the IMS network interfaces to the emergency services network, the emergency services network architecture is out of scope and is shown for informational purposes. For simplicity, the Common IMS Network shown does not include all IMS network elements. The Common IMS Network supports a variety of access types with mobile, nomadic, or fixed user equipment. The Common IMS Network delivers each call to either a legacy emergency services network or a NENA i3 ESInet. Calls destined for a legacy emergency services network are delivered from a Media Gateway Control Function (MGCF) to a Selective Router.

⁵ ATIS-0700015.v003, Applying common IMS core elements to ESInet architecture

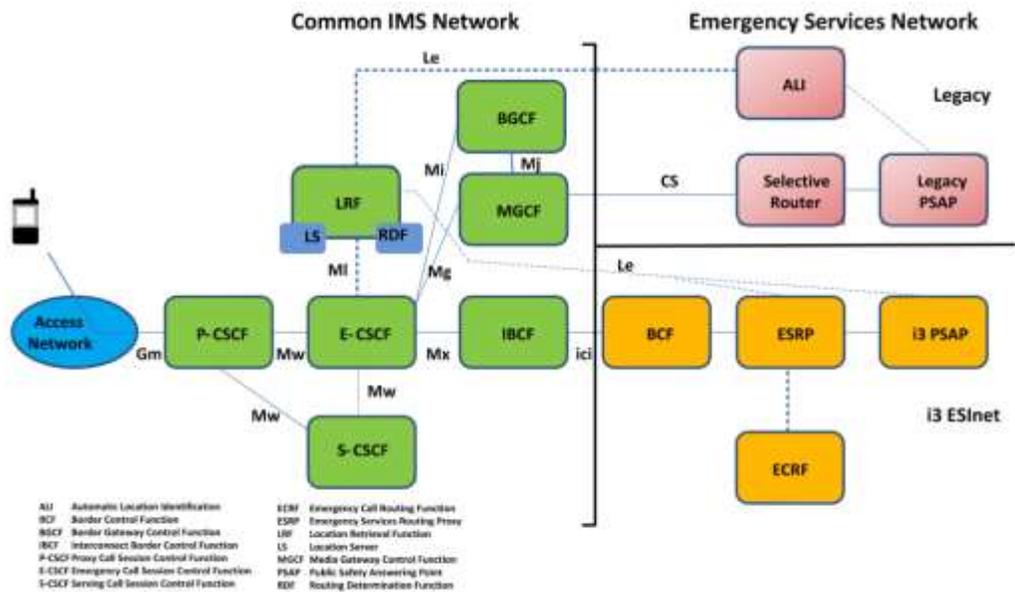


Figure 2 - IMS to ESInet diagram

It is important to consider the inclusion of IMS based systems, such as those already deployed by national carriers in the United States, and the integration of those systems into both legacy and NG9-1-1 infrastructures. While the IMS to ESInet standard is generally complimentary to the i3 approach, there are enough differences that WG1 believes public safety leaders should include IMS based systems and elements in their decision making process. Additionally, as FirstNet will be an IMS based system, comprised of multiple ESInets and will interface directly and indirectly with PSAPs at an operational level, cybersecurity planning which includes consideration of IMS elements is crucial.

4 Recommended Best Practices for Cybersecurity in both Transitional and Fully Deployed NG9-1-1 Systems

4.1 NIST Cybersecurity Framework (NCF)

The NCF 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. These activities are 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 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.

Working Group 1 has mapped out the recommended level of operation that should be involved in each of the five key areas identified in the NCF. In the Figure5 below, the working group has detailed both the recommended level for implementation and high-level requirements to achieve implementation at the appropriate level.

Function Unique Identifier	Function	Category Unique Identifier	Category	Implementation Level	Recommended Action Plan
ID	Identify	ID.AM	Asset Management	PSAP or 911 Authority	Inventory all resources throughout systems internally and externally. This should include at a minimum all data, hardware, software, and networks.
		ID.BE	Business Environment	PSAP or 911 Authority	Identify and document functions, processes, and entities within the support structure of your systems. This would include contracts, business agreements, mutual aide agreements, purchasing processes, service providers, vendors, contractors, etc.
		ID.GV	Governance	PSAP or 911 Authority	Identify and document applicable jurisdictional requirements, laws, regulations, or standards regarding the systems or functions they support.
		ID.RA	Risk Assessment	PSAP or 911 Authority	Evaluate the data gathered, Identify Business and Governance constraints, Categorize data and resources, Identify what is to be protected.
		ID.RM	Risk Management Strategy	PSAP (or 911 Authority) and EC3	Documentation of the policies, procedures, and controls are necessary to ensure completeness, facilitate training, and measure effectiveness. This should include the creation of response plans, recovery plans, continuity of operations plans, data destruction plans, data retention policies, and technical configurations.
PR	Protect	PR.AC	Access Control	PSAP or 911 Authority	Using the output of the risk assessments, vulnerability management data, and information security requirements establish the correct security controls for the environment.
		PR.AT	Awareness Training	PSAP or 911 Authority	Implement awareness and training program policy. This should be developed to include and consider roles and responsibilities. Use multiple channels to communicate the program.
		PR.DS	Data Security	PSAP (or 911 Authority) and EC3	Data should be protected in transit and at rest if deemed critical or sensitive. This can be done through various methods and systems using encryption and various other security controls.
		PR.IP	Information Protection Proc. & Proc.	PSAP or 911 Authority	Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
		PR.MA	Maintenance	PSAP or 911 Authority	Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.
		PR.PT	Protective Technology	EC3	Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements. Technologies should include at a minimum strong authentication processes, hardening of systems, firewalls, border control functions at ingress and egress points of the networks, encryption, intrusion detection, intrusion prevention, antivirus, anti-malware, bandwidth shaping, access control lists, etc.
DE	Detect	DE.AE	Anomalies and Events	EC3	Record and communicate to the appropriate and identified channels anomalies and events that exceed predetermined thresholds. Those identified channels will determine if a response is needed based on the information relayed.
		DE.CM	Security Continuous Monitoring	EC3	The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.
		DE.DP	Detection Processes	EC3	Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.
RS	Respond	RS.RP	Response Planning	EC3	Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.
		RS.CO	Communications	EC3	Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.
		RS.AN	Analysis	EC3	Evaluate the data gathered from the detection and protection systems. Analysis is conducted to ensure adequate response and support recovery activities.
		RS.MI	Mitigation	EC3	Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.
		RS.IM	Improvements	EC3	Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.
RC	Recover	RC.RP	Recovery Planning	EC3	Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.
		RC.IM	Improvements	EC3	Recovery planning and processes are improved by incorporating lessons learned into future activities. Documented issues or difficulties identified during the recovery process are added into the Risk Management Strategy.
		RC.CO	Communications	EC3	Recovery activities are communicated to internal stakeholders and executive and management teams.

Figure 3 - NIST Framework Core with Implementation Levels

4.2 Security Considerations for Apps interfacing to/with public safety

NIST hosted a half-day workshop earlier this year and has released a summary document reflecting input from attendees such as public safety practitioners, mobile application developers, industry experts, and government officials, who contributed their experience and knowledge to a discussion identifying security requirements for public safety mobile applications.⁶ The NIST summary is offered only as reference and does not represent any endorsement by WG1 of the work product. Much more work needs to be done in the defining these requirements and appropriate metrics and safeguards if mobile device apps are to be connected into and allowed to interface with public safety networks.

4.3 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 implementation model (FICAM).

The FICAM information detailed in the following section is derived, or directly sourced, from Federal ICAM documents⁷ 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.

—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.

4.3.1 ICAM Goals and Objectives

The goals and objectives in this section were created as part of the ICAM segment architecture development effort. While they primarily focus on the role of the Federal Government in achieving the ICAM end-state, other key stakeholders have a crucial role in enabling interoperability and trust across the ICAM landscape to accomplish secure information sharing outside of the Federal Government boundaries. These stakeholders, include external business and commercial entities wishing to conduct business with the Federal Government and state, local, and tribal governments that require information exchanges to meet mission needs.

4.3.2 ICAM Intersection

Understanding that ICAM programs have many areas of overlap is crucial to the overall success of these programs. There are many common elements associated with each of the areas addressed in the previous sections, including physical and logical access components, digital identities and attributes along with the systems that store them, and the workflow solutions that enable strong and dynamic processes. In fact, one of the primary dependencies across both the

⁶ Public Safety Mobile Application Security Requirements, Workshop (insert date), available at <http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8018.pdf>.

⁷

http://www.idmanagement.gov/sites/default/files/documents/FICAM_Roadmap_and_Implementation_Guidance_v2%200_20111202_0.pdf

credentialing and the access control environments is the presence of accurate identity and attribute information necessary to bind the digital representation of an entity to a credential, user accounts, and access privileges. (While access can be granted based on provisioned identifiers, roles, other attributes or policy based decisions based on several contextual data points, the access decision must correspond to the correct digital identity.)

As the necessity to complete transactions across networks with higher levels of assurance increases, so too does the need for the identity to be tied strongly and simultaneously to its high assurance credential, authoritative attributes, and access privileges. These overlaps demonstrate the intersection of identity, credential, and access management. Due to the size and complexity of the programs and functions related to ICAM, the following challenges have emerged to the adoption of a consistent approach to ICAM implementation, including:

- Lack of standardized terminology. The traditionally stove-piped nature of ICAM initiatives has driven community-specific definitions.
- Pressure to decrease redundant processes, data stores, and IT investments while increasing efficiency.
- Demand associated with quickly increasing the ROI associated with any ICAM infrastructure investment.
- Dependency on other organizations to adopt enabling technologies and processes that would enable secure cross-use of credentials and identity data.
- Need to establish impromptu areas that securely manage accurate identification and access control in order to accommodate emergency response scenarios.
- Differing levels of maturity for policies, processes, and technologies across departments and agencies who share common business needs

The goals and priorities of each agency vary and therefore affect the rigor in which ICAM goals are addressed. The first step to addressing these challenges is to view ICAM holistically instead of viewing it as separate disciplines. The same is true of the existing stove-piped programs across the Federal Government that have been implemented to address separate, but related initiatives. A comprehensive, coordinated approach to ICAM will help to resolve the significant IT, security, and privacy challenges facing multiple levels of government.

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.

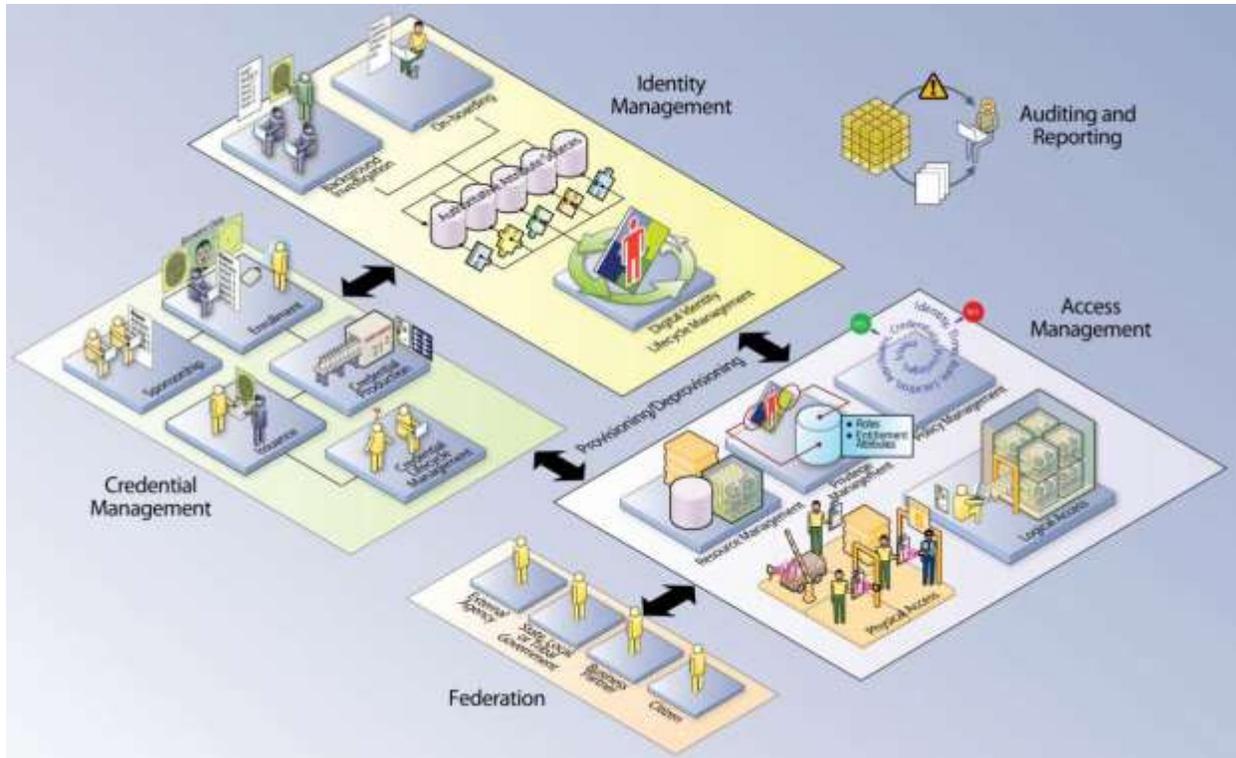


Figure 4 - ICAM "Big Picture"

4.3.3 FICAM Roadmap and Implementation Guidance

The Federal ICAM roadmap outlines strategic vision for identity, credential, and access management efforts within the Executive Branch of the Federal Government and demonstrates the importance of implementing the ICAM segment architecture in support of five overarching goals and the related objectives. These goals and objectives are listed in the figure below.



Figure 7 - Federal ICAM Roadmap

4.3.4 Value Proposition

The ICAM segment architecture establishes the foundation for trust and interoperability in conducting electronic transactions both within the Federal Government and with external organizations. It encompasses the core capabilities to be able to identify, authenticate, and authorize individuals to provide appropriate access to resources, which is the lynchpin to the success of the national cybersecurity initiative.



Figure 5 - Levels of Identity Assurance

4.3.5 Identity Management

Identity management is the combination of technical systems, policies, and processes that create, define, govern, and synchronize the ownership, utilization, and safeguarding of identity information. The primary goal of identity management is to establish a trustworthy process for assigning attributes to a digital identity and to connect that identity to an individual. Identity management includes the processes for maintaining and protecting the identity data of an individual over its life cycle. Additionally, many of the processes and technologies used to manage a person's identity may also be applied to Machine to Machine (M2M) to further security goals within the enterprise.

As part of the framework for establishing a digital identity, proper diligence should be employed to limit data stored in each system to the minimum set of attributes required to define the unique digital identity and still meet the requirements of integrated systems. A balance is needed between information stored in systems, information made available to internal and external systems, and the privacy of individuals. In the context Public Safety and 9-1-1 Authority operations, this equates to the establishment of an enterprise identity, defined as the Public Safety Enterprise network. This is key from the PSAP level up through any proposed cybersecurity core architecture and into the Federal space. From the local perspective, this

would involve the physical verification of an individual to be granted access, usually done as part of the onboarding and background check process, and issuance of a user name, password and some form of token or additional authentication mechanism. This approach is commonly referred to as multi-factor authentication and it is highly recommended that it be implemented in each PSAP, along with defined interfaces from the PSAPs to any core NG9-1-1 services, to ensure uniform, controlled, and protected access. The following section discusses credential and access management in more detail.

4.3.6 Credential Management

According to NIST Special Publication 800-63 (NIST SP 800-63), a credential is, an object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person. Examples of credentials are smart cards, private/public cryptographic keys, and digital certificates. The policies around credential management, from identity proofing to issuance to revocation, are fairly mature compared to the other parts of ICAM.

4.3.7 Access Management

Access management is the management and control of the ways in which entities are granted or denied access to resources. The purpose of access management is to ensure that the proper identity verification is made when an individual attempts to access security sensitive buildings, computer systems, or data. It has two areas of operations: logical and physical access. Logical access is the access to an IT network, system, service, or application. Physical access is the access to a physical location such as a building, parking lot, garage, or office. Access management leverages identities, credentials, and privileges to determine access to resources by authenticating credentials.

Logical and physical access are often viewed as the most significant parts of ICAM from a return on investment (ROI) perspective. To maximize that return, a successful access management solution is dependent on identity, credentials, and attributes for making informed access control decisions, preferably through automated mechanisms. This approach enables an Access Management initiative to promote security and trust and meet business needs while achieving the envisioned value.

5 NICE Workforce Framework

The National Initiative for Cybersecurity Education (NICE) developed a National Cybersecurity Workforce Framework (Workforce Framework) to define the cybersecurity workforce and provide a common taxonomy and lexicon by which to classify and categorize workers. The Workforce Framework lists and defines specialty areas of cybersecurity work and provides a description of each. Each of the types of work is placed into one of seven overall categories. The Workforce Framework also identifies common tasks and knowledge, skills, and abilities (KSA's) associated with each specialty area.⁸

Workforce planning is a systematic way for organizations to determine future human capital requirements (demand), identify current human capital capabilities (supply), and design

⁸ A comprehensive application of the Workforce Framework is beyond the scope of this working group. Reference material and additional tools for the Workforce Framework can be found on the National Initiative for Cybersecurity Careers and Studies (NICCS) website found at: <https://niccs.us-cert.gov/training/tc/framework>

and implement strategies to transition the current workforce to the desired future work state. Effective workforce planning highlights potential risk areas associated with aligning the workforce to work requirements. Applied correctly, workforce planning allows organizations to adjust resources to meet future workloads, patterns of work, and fundamental changes in how work is accomplished. A workforce planning approach must fit the needs of a specific organization and account for unique characteristics of the cybersecurity profession. An example workforce planning process is illustrated below:

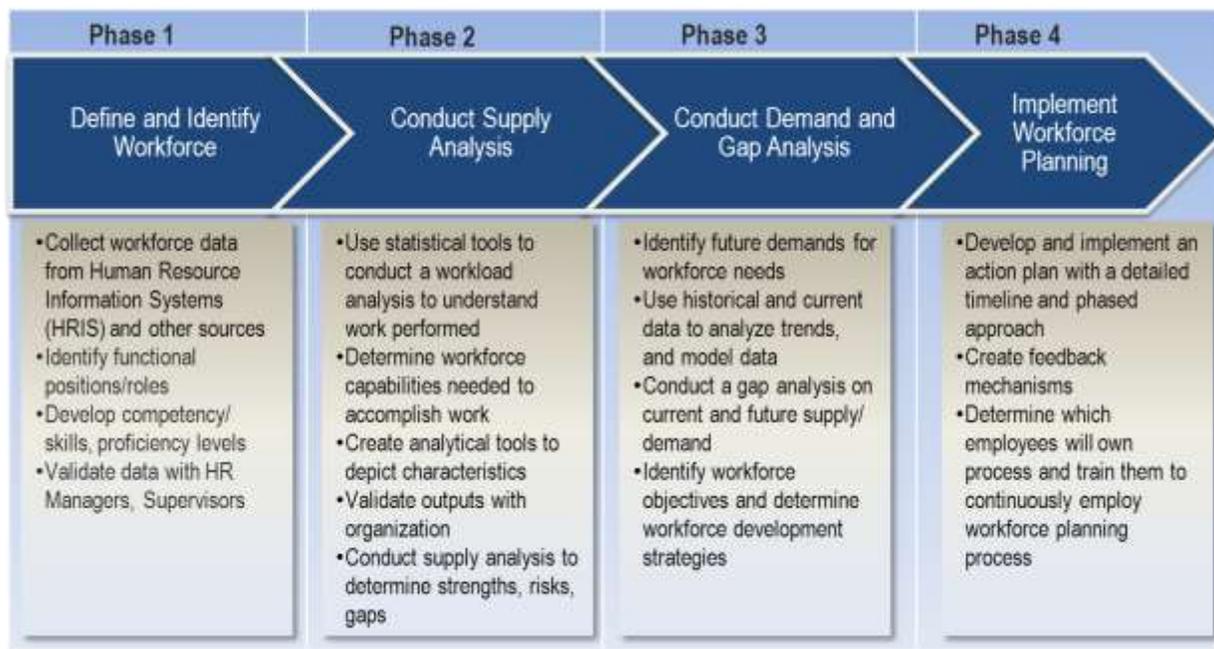


Figure 6 – Workforce Planning Process

The first step in workforce planning, Define and Identify, emphasizes the collection of workforce data that defines the workforce and the identification of positions/roles within the workforce with specific role based competencies and proficiency levels. This activity in turn establishes the knowledge, skills, and abilities (KSAs) that are the attributes required to perform a job and are generally demonstrated through qualifying experience, education, or training.

As a prescriptive example to Define and Identify Workforce, the working group members reviewed job titles, roles and skills to assess NICE Framework labor categories, scope of work, and information technology skills most closely associated with each. While PSAPs generally do not have a single consistent model for job titles, a generalized set of job titles were mapped to labor categories with identification of required skills and recommended training based on the NICE Workforce Framework. The results are captured in the Table below as a baseline example of application of the Workforce Framework to Public Safety:

<u>PSAP job titles:</u>	<u>Category</u>	<u>Scope of Work</u>	<u>Required Skills (IT Related)</u>	<u>Example Training</u>
Director/Administrator	Oversight and Development	Administer the telecommunications and Emergency Medical Dispatch functions of the Bureau of Emergency communications thru planning both short and long term goals. Analyze and develop staffing plans based on historical data in order to revise or develop operational policies and procedures.	Operates computers and AV equipment as needed.	Cyber Hygiene Cyber Security for Managers
Deputy Director, Operations Manager, Technical Manager, Radio Systems Manager	Oversight and Development	Direct support to the Director/Administrator in the management of the telecommunications and Emergency Medical Dispatch functions of the Bureau of Emergency communications thru planning both short and long term goals. Analyze and develop staffing plans based on historical data in order to revise or develop operational policies and procedures. Dependent on organization of the department/agency, deputy directors may have specific responsibilities involving one or more of operations, technology, training, radio networks and systems, quality assurance.	Operates computers and AV equipment as needed. Additional system specific IT skills driven by organizational responsibility that would define specific scope of additional recommended training.	Cyber Hygiene Cyber Security for Managers - Network + - Security + - IR Framework - CISSP
Administrative Assistant	Administrative support	Under the supervision of the Director, performs a variety of administrative support tasks and reviews and processes warrants. Drafts and types various correspondence, maintains accounting records, gathers data and prepares reports. Attends meetings and takes minutes.	Operates computers and AV equipment as needed.	Cyber Hygiene
Case Review & Evaluation Specialist/Quality Assurance Manager	Oversight and Development	Provides assistance to the Emergency Medical Service (EMS) Medial Control Board in determining if correct protocol was used in handling of medical calls, respond to complainants, and to serve as a liaison between the Medical Control Board, the Bureau of Emergency Communication and all public safety emergency agencies.	Operates computers and AV equipment as needed.	Cyber Hygiene Cyber Security for Managers
Data Processing Supervisor, MSAG Coordinator /Location Services Administrator, Field Representative	Oversight and Development	Summarize the collection and verification of location data and make recommendations for inclusion in the E9-1-1 and NG-9-1-1 transition of telephone and GIS databases. Checks and monitors accuracy of GIS data collected in the field. Performs data comparisons to sync telephone and GIS databases. Accomplish and maintain a mapping database to be used for emergency response directions.	Operates computers and AV equipment as needed. Uses database management systems. Monitors calls for addressing accuracy and initiates reports of incorrect information to assure database update	Cyber Hygiene Cyber Security for Managers - Security +

<u>PSAP job titles:</u>	<u>Category</u>	<u>Scope of Work</u>	<u>Required Skills (IT Related)</u>	<u>Example Training</u>
Public Safety Answering Point Supervisor	Oversight and Development	Supervises subordinate field representative employees (dispatchers, call takers, and/or telecommunicators; see below) in the daily operations of their sections to achieve agency objectives. Responsible for understanding the technologies and workflows for the data operations support section.	Operates computerized the phone system for E9-1-1, NG9-1-1. Operation of TTY/TDD Operation of Text 9-1-1 systems Monitors 9-1-1 data to get real-time information about emerging threats.	Cyber Hygiene Cyber Security for Managers
Police, Fire, EMS Dispatcher / 9-1-1 Call Taker / Public Safety Telecommunicator	Operate and Maintain	Operate emergency telecommunications computerized console system, to receive, assess, make judgment, and forward to appropriate emergency service providers emergency requests for police, fire or medical assistance. Provide life sustaining instructions for medical patients until the arrival of responding medical personnel. Follows strict Division, state, and national standards and policies.	Operates computerized the phone system for E9-1-1, NG9-1-1. Operation of TTY/TDD Operation of Text 9-1-1 systems Monitors 9-1-1 data to get real-time information about emerging threats.	Cyber Hygiene Cyber Security for Managers
Public Information Representative	Operate and Maintain	Create and Maintain a media campaign to educate the public about E-9-1-1	Operates computers and AV equipment as needed.	Cyber Hygiene
Training Coordinator	Oversight and Development	Plan, develop, and monitor training programs in a variety of Emergency communications related classes in order to maintain an enhanced service to the public. Review supervisors and Telecommunications Specialists work performance, perform annual evaluations on supervisory and training staff and make recommendations for salary increases.	Training programs for PSAP staff to maintain proficiency and ensure conformance to standards maintains employee training records for certification and performance Administers in-house testing and leads interview panel for selected applicants	Cyber Hygiene Cyber Security for Managers

<u>PSAP job titles:</u>	<u>Category</u>	<u>Scope of Work</u>	<u>Required Skills (IT Related)</u>	<u>Example Training</u>
GIS Administrator	Operate and Maintain	Manages GIS objectives by authorizing and directing implementation of policies and procedures to meet long term strategies. Analyzes, develops, and approves applications for grant funds to support new GIS tech. Develops and manages GIS projects as assigned.	Authorizes the development of statewide advanced GIS policies, goals and objectives Monitors operational activities for efficient and effective allocation of resources. Manages personnel in the Special Operations section Coordinates interagency GIS data transfer and maintenance Manages the design, development, and maintenance of custom software for DESC special operations	Cyber Hygiene - Security +
GIS Technicians/ Cartographers	Operate and Maintain	Performs public safety and ER mapping activities utilizing geospatial tools and equipment to support division.	Develops and maintains GIS components Provides data management for GIS components Recommends policies and procedures Supervises and trains employees in the use of various GIS systems Utilizes a variety of databases	Cyber Hygiene - Security +
IT Manager/Director	Oversight and Development	Administers all aspects of agency-wide technology solutions in support of the agencies core and ancillary functions under the direction of Division Director. Senior IT manager for the Technical Support Unit. Manages all aspects of agency data operations including 9-1-1 Telephone Database, 9-1-1 GIS Database, and implementation of NG9-1-1 and the ENS.	Authorizes Policies and Procedures for design and administration of Databases. Plans and Evaluates E9-1-1 HW & SW solutions. Evaluates trends in communications. Makes recommendations on HW&SW Directs assigned managers and supervisors to coordinate team resources. Evaluates IT & IP communications to ensure productivity of assigned resources	Cyber Hygiene Cyber Security for Managers - Network + - Security + - IR Framework - CISSP

<u>PSAP job titles:</u>	<u>Category</u>	<u>Scope of Work</u>	<u>Required Skills (IT Related)</u>	<u>Example Training</u>
Network Administrator	Operate and Maintain	Network and computer systems administrators are responsible for the day-to-day operation of voice and data networks. They organize, install, and support an organization's computer systems, including local area networks (LANs), wide area networks (WANs), network segments, intranets, and other data communication systems.	Network and computer system operating systems, router configurations, IP and other communications protocol stacks, access control systems, network encryption (VPN, SSL, etc.), network monitoring	Cyber Hygiene - Network + - Security + - IR Framework - CISSP
PC Technician, Systems Technician, Network Technician, Radio Technician	Operate and Maintain	They install, configure and maintain the hardware and software that comprise voice and data communications networks. May be responsible for network components, client workstations, servers, domain controllers, shared printers, cables, and routers, radio system controllers, RF network components, cable and fiber systems and other related communications systems. They maintain network equipment, applications, data and user interfaces and workstations as well as troubleshoot local and wide area networks.	Computer system hardware and software configuration, maintenance, and troubleshooting, Land Mobile Radio equipment configuration, maintenance and troubleshooting	Cyber Hygiene - Network + - Security + - IR Framework
Database Administrator	Operate and Maintain	Responsible for the performance and security of databases. The role includes the development and design of database strategies, system monitoring and improving database performance and capacity. They may also plan, co-ordinate and implement security measures to safeguard the database	Computer system hardware and software configuration, maintenance, and troubleshooting. Specific skills focus on database architecture, application development, system backup and recovery, and database performance indexing.	Cyber Hygiene - Security +
Senior Technical Coordinator	Operate and Maintain	Designs, plans, and implements agency wide technology solutions in support of the agency functions under the direction of the IT manager. Interfaces with vendors IT resources to develop plan and implement installations and upgrades. Serves as a technical resource for junior staff and conducts in-house training.	Computer system hardware and software, network hardware and software, IP and other protocol stacks, system and network monitoring and performance management	Cyber Hygiene - Network + - Security + - IR Framework - CISSP
Technical Support Specialist	Operate and Maintain	Maintain current and future information technology systems, evaluate and develop system procedures, resolve system problems and assist in the development of training for users in a computer environment.	backup and restore - COOP plan Implements agency use and security policies and reviews for compliance monitors, projects, and analyzes network performance Coordinates with IT staff to troubleshoot, enable, or limit WAN/LAN connectivity	Cyber Hygiene - Network + - Security + - IR Framework

Table 2 - NICE Framework mapping for Public Safety

5.1 *DHS recommendations and resources*

WG1 representatives from the U.S. Department of Homeland Security (DHS) contributed the following section. DHS offers a number of optional programs and solutions for consideration by the public safety community. While the following is included in the report, it does not represent an endorsement of any specific program or project.

DHS is committed to increasing the cybersecurity posture of the public safety community and resiliency of communications networks. The Department is working with the public safety community to identify opportunities to leverage DHS' cybersecurity capabilities to provide best practices and conduct analyses aimed at the unique challenges of State Emergency Operations Centers (EOCs), PSAPs, and other critical infrastructure.

5.1.1 Technical Programs

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.

Cybersecurity Operations. The NCCIC⁹ is a 24/7 cyber monitoring, incident response, and management center. Organizations can leverage NCCIC's United States Computer Emergency Readiness Team (US-CERT) for cybersecurity information and assistance. US-CERT hosts the National Cyber Awareness System (NCAS), which offers a free, publicly available set of cybersecurity data including emerging threat data, alerts and reports.¹⁰

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 Communication1 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 cyber security 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 operations.¹¹ Additionally, DHS manages the Emergency Services Sector (ESS) Cyber Working Group to evaluate cyber risks that the sector might encounter.¹²

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, Cyber Risks to Next Generation 9-1-1.¹³ 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

⁹ NCCIC/National Coordinating Center for Communications (NCCIC/NCC) is the federal lead organization for Coordination of the Stafford Act's National Response Framework ESF-2, (Communications) and is also the Communications ISAC, with cleared industry representatives from APCO, NENA and major carriers, such as AT&T, Verizon, Century Link, Sprint and T-Mobile

¹⁰ National Cyber Awareness System, <https://www.us-cert.gov/ncas>.

¹¹ Office of Emergency Communications, <http://www.dhs.gov/office-emergency-communications>.

¹³ Cyber Risks to Next Generation 9-1-1, available at <http://www.dhs.gov/office-emergency-communications>.

Internet Protocol (IP) Emergency Services Sector Cyber Risk Assessment¹⁴ and Emergency Services Sector Roadmap to Secure Voice and Data Systems¹⁵ 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 NCCIC to automate cybersecurity information sharing amongst its members.¹⁶

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.¹⁷ DHS also supports the National Initiative for Cybersecurity Education (NICE), which provides additional educational resources for public and private organizations.¹⁸ DHS also delivers education and technical assistance to Federal, State and local public safety community on PSAP deployments.

Outreach and Assistance. The Critical Infrastructure Cyber Community C³ (pronounced “C Cubed”) Voluntary Program (C³VP) 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. C³VP can assist PSAPs in understanding how to use NIST’s Cybersecurity Framework and other risk management efforts.

5.1.2 Technical Solutions

DHS offers a collection of programs and initiatives that can be applied to reduce NG9-1-1 cyber risks. Many of these efforts support missions that cover State and local users, as well as public and private critical infrastructure entities. In some instances, technical solutions may only apply to Federal organizations, however the methodology can be applied to most NG9-1-1 PSAP networks and can provide cost savings in addition to reducing cyber risk.

Solution	Description
Trusted Internet Connection	Works to enable organizations to identify and consolidate Internet connections (http://www.dhs.gov/trusted-internet-connections). As content and applications move to public cloud providers, CS&C is collaborating with the Federal Risk and Authorization Management Program (FedRAMP) to apply a TIC

¹⁴ 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>

¹⁵ESS 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>

¹⁶ (<https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity>)

¹⁷ (<http://www.dhs.gov/stopthinkconnect>)

¹⁸ (<http://csrc.nist.gov/nice/index.htm>)

(TIC) ¹⁹	approach(https://www.fedramp.gov/draft-fedramp-tic-overlay/)
Network Flow Collection	Provides the enterprise with an awareness of the type and volume of traffic flowing into (and out of) the enterprise network. Information includes source/destination IP address, domains, and ports. This data can be filtered and searched to identify anomalous flow patterns, and initiate further research into potential risks and attacks. Flow collectors are deployed at TIC locations, supporting Federal and State stakeholders. (https://msisac.cisecurity.org/about/services/)
Intrusion Detection (IDS)	DHS provides IDS sensors at TIC locations, and also develops digital signatures which are loaded into the IDS to identify threats. Organizations receiving this service are able to view alerts created by the IDS (occurring when signatures identify pattern matches in network traffic). This service is currently available to Federal and State stakeholders. (http://www.dhs.gov/cybersecurity-and-privacy)
Intrusion Prevention (IPS)	DHS deploys IPS to public and private network owners. IPS is similar to IDS in that digital signatures are used at the sensor. With IPS, when signatures identify pattern matches, countermeasure actions are taken such as dropping or rerouting traffic. While network flow collection and IDS are passive (i.e., monitoring and alerting) cybersecurity measures, IPS is an active security measure. (http://www.dhs.gov/cybersecurity-and-privacy)
Continuous Diagnostics and Mitigation (CDM)	DHS deploys CDM services, which include hardware and software asset management, configuration management, vulnerability management capabilities. These services are enabled through devices (physical and virtual) deployed inside the enterprise network, and presented to security professionals in a dashboard. For stakeholder organizations (currently only Federal Civilian Agencies), CDM is the major technology solution that supports the tenets of ongoing authorization. (http://www.gsa.gov/portal/content/177895)
Risk Assessment and Risk Analysis	DHS provides infrastructure baseline assessments, vulnerability assessments, impact assessments, and comprehensive risk and mitigation analyses of public safety infrastructure and services in conjunction with other departments and agencies, as well as individual PSAPs.

5.2 CSRIC Best Practices Related to Public Safety

The Communications Security, Reliability, and Interoperability Council (CSRIC) was established as a federal advisory committee designed to provide recommendations to the Federal Communications Commission regarding best practices and actions the Commission can take to ensure optimal security, reliability, and interoperability of communications systems, including telecommunications, media and public safety communications systems. CSRIC created ten working groups, each with its own area of responsibility.

CSRIC IV Working Group 4 (WG4) was tasked with developing voluntary mechanisms that give the Commission and the public assurance that communication providers are taking the necessary measures to manage cybersecurity risks across the enterprise.²⁰ WG4 also was charged with providing implementation guidance to help communication providers use and adapt the NCF. WG1 supports the use of NIST CFS as recommendation as they apply in the final WG4 report. Readers should pay special attention to barriers of implementation within that report. Since each implementation may have its own specific challenges of note would be potential barriers with respect to technology, scale, consumers, marketplace entry, law or policy.

²⁰ The report is available at:
https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf

6 Proposed Approaches to NG9-1-1 Cybersecurity Architecture

6.1 The Emergency Communications Cybersecurity Center (EC3)

In addition to incorporating current best practices, NIST recommendations, and current work from DHS, APCO, ATIS and NENA the working group has determined that an additional layer should be introduced into the recommended future architecture.

The intent of this logical architecture recommendation is to create a centralized function, and location, for securing NG networks and systems. By centralizing certain features, including cybersecurity in general, and intrusion detection and prevention services (IDPS) specifically, public safety can take advantage of economies of scale, multiple resources, and systems and best practices which may already be in place or at a minimum readily available for deployment and use.

This section is intended to empower local, state, tribal and territorial PSAP and 9-1-1 authority leaders, by providing information and enumerating options to allow leadership to make informed decisions on how to implement a cybersecurity plan and infrastructure best suited for their agencies and needs. The establishment of certain shared core services like cybersecurity, which can be utilized by multiple participating agencies, can produce substantial cost savings for each participating agency and could also decrease the time needed to implement a comprehensive cybersecurity system for PSAPs and 9-1-1 authorities. In sharing this portion of NG9-1-1 infrastructure, PSAPs decrease the amount of work and specialization needed at the local level, and can instead take advantage of centralized, expert cybersecurity services allowing them to concentrate on the life-saving, day-to-day operations related to taking and dispatching calls for service.

6.2 Description of Intrusion Detection and Prevention Systems

In order to function effectively as a tool for public safety and emergency communications systems, the EC3 must perform all of the essential functions of a comprehensive Intrusion Detection and Prevention System. The following is a high level description of those desired features and functions.

IDPSs are primarily focused on identifying possible incidents. For example, an IDPS could detect when an attacker has successfully compromised a system by exploiting a vulnerability in the system. The IDPS could then report the incident to security administrators, who could quickly initiate incident response actions to minimize the damage caused by the incident. The IDPS could also log information that could be used by the incident handlers. Many IDPSs can also be configured to recognize violations of security policies. For example, some IDPSs can be configured with firewall ruleset-like settings, allowing them to identify network traffic that violates the organization's security or acceptable use policies. Also, some IDPSs can monitor file transfers and identify ones that might be suspicious, such as copying a large database onto a user's laptop.

Many IDPSs can also identify reconnaissance activity, which may indicate that an attack is imminent. For example, some attack tools and forms of malware, particularly worms, perform reconnaissance activities such as host and port scans to identify targets for subsequent attacks. An IDPS might be able to block reconnaissance and notify security administrators, who can take actions if needed to alter other security controls to prevent related incidents. Because

reconnaissance activity is so frequent on the Internet, reconnaissance detection is often performed primarily on protected internal networks.

There are many types of IDPS technologies, which are differentiated primarily by the types of events that they can recognize and the methodologies that they use to identify incidents. In addition to monitoring and analyzing events to identify undesirable activity, all types of IDPS technologies typically perform the following functions:

Recording information related to observed events. Information is usually recorded locally, and might also be sent to separate systems such as centralized logging servers, security information and event management (SIEM) solutions, and enterprise management systems.

Notifying security administrators of important observed events. This notification, known as an *alert*, occurs through any of several methods, including the following: e-mails, pages, messages on the IDPS user interface, Simple Network Management Protocol (SNMP) traps, syslog messages, and user-defined programs and scripts. A notification message typically includes only basic information regarding an event; administrators need to access the IDPS for additional information.

Producing reports. Reports summarize the monitored events or provide details on particular events of interest.

Some IDPSs are also able to change their security profile when a new threat is detected. For example, an IDPS might be able to collect more detailed information for a particular session after malicious activity is detected within that session. An IDPS might also alter the settings for when certain alerts are triggered or what priority should be assigned to subsequent alerts after a particular threat is detected.

IPS technologies are differentiated from IDS technologies by one characteristic: IPS technologies can respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which can be divided into the following groups:

- **The IPS stops the attack itself.**
 - Will terminate the network connection or user session that is being used for the attack
 - Block access to the target (or possibly other likely targets) from the offending user account, IP address, or other attacker attribute
 - Block all access to the targeted host, service, application, or other resource
- **The IPS changes the security environment.**
 - IPSs Can change the configuration of other security controls to disrupt an attack by reconfiguring a network device (*e.g.*, firewall, router, switch) to block access from the attacker or to the target
 - Alters a host-based firewall on a target to block incoming attacks.
 - Some IPSs can even cause patches to be applied to a host if the IPS detects that the host has vulnerabilities.
- **The IPS changes the attack's content.**
 - Some IPSs can remove or replace malicious portions of an attack to make it benign (*e.g.*, removing an infected file attachment from an e-mail and then permitting the cleaned email to reach its recipient).
 - Other IPSs act as a proxy and *normalizes* incoming requests, which means that

the proxy repackages the payloads of the requests, discarding header information. This might cause certain attacks to be discarded as part of the normalization process.

Another common attribute of IDPS technologies is that they cannot provide completely accurate detection. When an IDPS incorrectly identifies benign activity as being malicious, a *false positive* has occurred. When an IDPS fails to identify malicious activity, a *false negative* has occurred. It is not possible to eliminate all false positives and negatives; in most cases, reducing the occurrences of one increases the occurrences of the other. Many organizations choose to decrease false negatives at the cost of increasing false positives, which means that more malicious events are detected but more analysis resources are needed to differentiate false positives from true malicious events. Altering the configuration of an IDPS to improve its detection accuracy is known as *tuning*.

Most IDPS technologies also offer features that compensate for the use of common evasion techniques. Evasion is modifying the format or timing of malicious activity so that its appearance changes but its effect is the same. Attackers use evasion techniques to try to prevent IDPS technologies from detecting their attacks. For example, an attacker could encode text characters in a particular way, knowing that the target understands the encoding and hoping that any monitoring IDPSs do not. Most IDPS technologies can overcome common evasion techniques by duplicating special processing performed by the targets. If the IDPS can “see” the activity in the same way that the target would, then evasion techniques will generally be unsuccessful at hiding attacks.¹

6.3 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 PSAPs and any other emergency communications service or system that would consider utilizing the centralized, core services architecture proposed. For example, not only PSAPs 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 PSAPs 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 PSAPs. Rather than requiring PSAPs to build and staff such facilities, the EC3 concept allows for PSAPs 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 PSAP, 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.

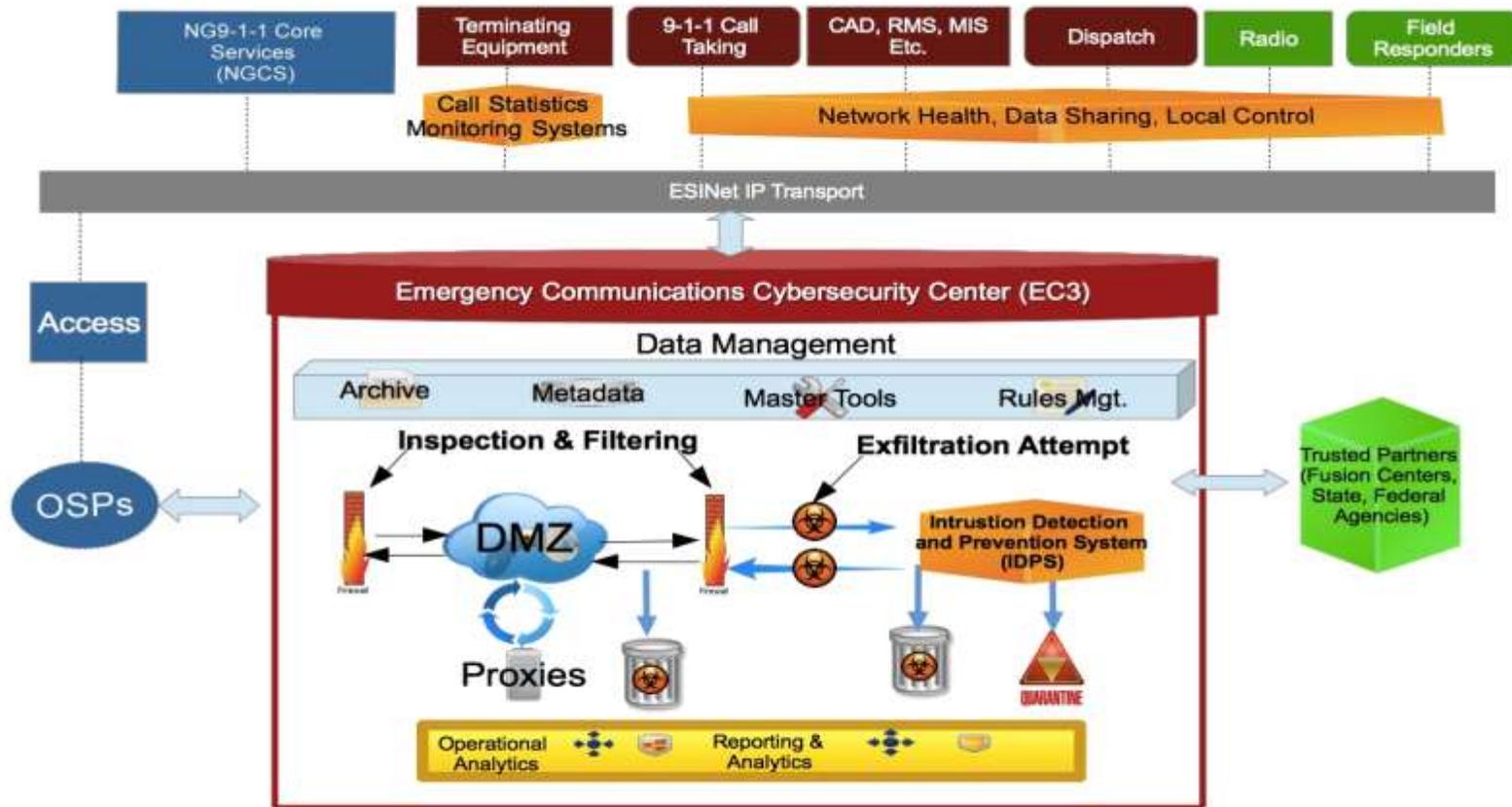


Figure 7 – Proposed Architecture for Emergency Communications Cybersecurity Center (EC3)

December, 2015

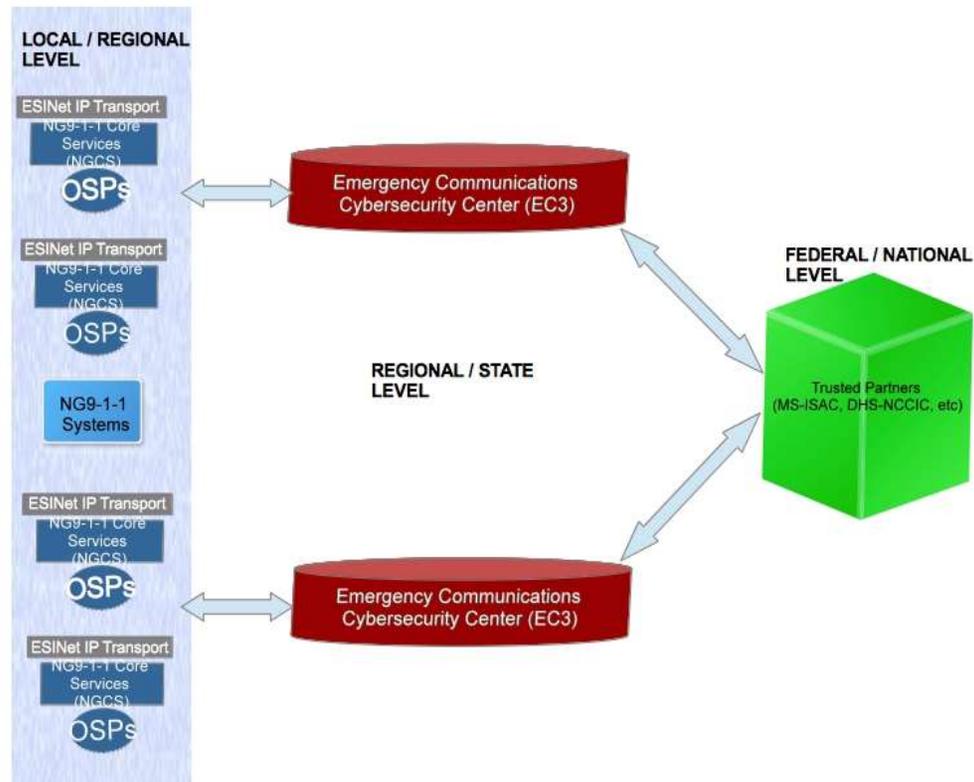


Figure 8 - EC3 Information Flow Example

6.3.1 The EC3 Concept Explained

The information collected by the EC3s that relates to the PSAPs 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 PSAP 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 WG1 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, WG1 received input and assistance from representatives of the MS-ISAC.²¹

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 PSAPs 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 PSAP 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 PSAPs.

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

²¹ More information about the MS-ISAC can be found at <https://msisac.cisecurity.org>.

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, both NCC members, proposed leveraging an existing sensor system deployed within PSAPs in California could be used to support a mission of protecting the PSAPs as an enterprise against cyber-attacks, physical disaster response and ensuring continuity of emergency communications.

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 PSAPs 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.

The NCCIC, in partnership with CalOES is capable of providing constant and continual monitoring of the ECATS dashboard, deployed by CalOES across the entire State of California. In this capacity the NCC and NCCIC can coordinate with CalOES, FBI, and other government agencies and telecommunications service providers in the event of an anomaly across one or many PSAPs. Additionally, use of this Local-State-Federal partnership model enables a coordinated, and unified, restoration effort in the event of loss of connectivity. This model also allows for monthly reports of incidents, and outcomes, along with investigative assistance and coordination of lessons learned via after action reports involving all stakeholders.

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 PSAPs 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 PSAPs 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 PSAPs 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 PSAPs.

Depending on the specific needs of the PSAPs, 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 a 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 PSAPs 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.

6.3.2 Cost Considerations

6.3.2.1 Operational Costs and Considerations

In order to run a basic EC3, supporting multiple PSAPs at a State or sub-State Regional level in a 24x7 capacity, the minimum amount of staff needed to do so is projected at five analysts and one manager. The manager should also act as a person-on-call so that issues after hours may be escalated as needed. As the operation grows and additional staffing is required, the operation can then add more people to the busier shifts. As a general rule of thumb, obtaining individuals with the education and experience needed to fulfill these roles will cost from between \$100,000 to \$150,000 per year per person. Using an average cost per employee of \$125,000 the very rough estimate as to operational, recurring costs to operate an EC3 will be approximately \$625,000 per year. Cost for benefits for these personnel range from between 18 to 30 percent on a nationwide average. Using a blended average of 24 percent, the approximate personnel costs of the center are \$775,000.

In addition, there will be costs for utilities, bandwidth, and communications, the need for sensors, potential annual costs for those elements, as well as recurring rent or taxes. The group has concluded that costs can vary from \$100,000 per year up to \$250,000 per year depending on the location of the center and the types of technologies chosen and the amount of bandwidth required. The working group suggests using an average of \$175,000 per year for all ancillary expenses that could be associated with the operation of an EC3. This provides a rough, rounded estimate of approximately \$950,000 per year in operating expense for an individual EC3. While it is not possible to definitively predict the cost for every individual EC3, as there are a number of variables, this average assumes one center that supports multiple PSAPs and is staffed 24 hours a day, 365 days a year. Larger centers, supporting larger geographic areas or in need of greater data capabilities and personnel will obviously incur additional cost. The suggested estimate is intended to provide a guideline, not a quote, to enable PSAPs and 9-1-1 Authorities to gauge potential cost sharing, and cost saving, options and make informed decisions.

Thanks to input from the MS-ISAC, the following is a breakdown of a typical monthly

service cost, based on the throughput of the network's Internet connection to be monitored. This information is provided for base reference purposes only and the working group is not suggesting, or endorsing, any specific product or product suite.

Pricing: Based on Internet Provisioned Connection Size.

One-time initiation fee of **\$850, per sensor**

Size up to 10MB - \$590/month

Size > 10MB-100MB- \$890/month

Size > 100MB-1GB- \$1,390/month

Size > 1GB - 10GB - \$2,790/month

6.3.2.2 Capital Costs and Considerations

The building out of the EC3 should be a very similar per foot cost as compared to the building out of normal office space which typically includes cubicles and workstations for analysts. There may be some additional costs incurred for flat panel displays and a computer system to drive them as well. As a result, while the working group cannot provide a high level estimate for what an EC3 physical build out might cost, as these costs may vary widely, the group does believe that the guidelines provided should allow local, regional, and State decision makers to have a starting point from which they can at least begin estimates based on local cost factors. When making such decisions, local organizations are encouraged to consider repurposing existing facilities or taking advantage of long-term lease options for space and operations in existing data or security centers.

In addition to building, repurposing, or co-locating at existing data and/or security centers, a physical buildout, and capital expense, will be necessary for the deployment of sensors at the EC3s. At a high level, it would make the most sense to deploy an "Albert like" sensor at each EC3, as the EC3s (ideally) would be the aggregation point of all PSAP network traffic. These sensors are essentially commodity hardware and typically cost between \$6,000 – \$12,000 depending on the throughput of the network that is being monitored. For example, a \$12,000 sensor would be more than capable of monitoring a 10GB network with an average utilization of 6-8GB. In addition, and as previously discussed, it would also be recommended that consideration be given to deployment of a sensor system similar to that used by CalOES. While the working group does not have price estimates for such a deployment, we believe they could be obtained by contacting CalOES officials directly.

6.3.2.3 Summary of Cost Considerations

As shown, there are substantial costs associated with building out the physical and network related architectures and operating and maintaining the systems that will support cybersecurity functions. Rather than suggesting that each of the more than 6,500 PSAPs in the United States be burdened with building and staffing such facilities, the working group believes utilizing core EC3's at various levels (Regions within a State, State level, or Regions comprised of multiple States and 9-1-1 authorities) can offer public safety both economies of scale and operational efficiencies. In addition, a cooperative approach on the cybersecurity front brings a greater number of resources to bear for any incident, provides small, medium, and large PSAPs with equal resources and capabilities to defend against, and recover from, cyber-attacks and allows for real time information sharing and intelligence. In addition, monitoring systems that are respectful of PII, such as those mentioned previously, will allow for the sharing of network

and system health without compromising the security of individuals or organizations.

WG1 believes that the high level estimates provided, based on existing deployments of a similar nature, provide a valid starting point for local leadership to assess need and potential costs, or cost sharing strategies. However, due to a somewhat limited timeline in which to complete the TFOPA report, the working group also believes additional research in this area, to include alternate technologies, existing vendors with similar solutions, and potential commercial and government partnerships in this endeavor is merited. To this end, working group one recommends additional study on costs, available solutions, and potential partnerships.

7 Recommendations

The Working Group's approach to these recommendations recognized that the local control is essential to any public safety related project at the State and Local level, and an architecture, or architecture options, balanced with the need to create a manageable core infrastructure which supports distributed network elements to the PSAP level is equally important.

- WG1 has determined that an additional layer should be introduced into the recommended future architecture. The intent of the logical architecture proposed in the form of the EC3 is to create a centralized function for securing NG networks and systems. By centralizing certain features, including cybersecurity in general, and intrusion detection and prevention services (IDPS) specifically, public safety can take advantage of economies of scale, multiple resources, and systems and best practices which may already be in place or at a minimum readily available for deployment and use.
- Cybersecurity Operations will require a 24x7x365 monitoring, incident response, and management approach. Local PSAPs, 9-1-1 Authorities and regional organizations can leverage a number of existing capabilities, such as the DHS NCC, NCCIC, MS-ISAC and existing State level Fusion centers for cybersecurity information and assistance. In addition, with the incorporation of the EC3 concept, all of these potential partners can be included in the holistic approach to cybersecurity which will allow local authorities to share costs while benefiting from more comprehensive services and capabilities that might otherwise be unavailable and most certainly could be cost prohibitive without a shared approach.
- Public / Private Collaboration is critical to the success of a comprehensive cybersecurity approach. 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 NCCIC to automate cybersecurity information sharing amongst its members. This is one example of how collaboration can be achieved and provides a model to build on. Again, the EC3 concept proposes that public safety at multiple levels (local, regional, State and Federal) cooperate in a number of different ways, both operational and financial, to achieve this goal.

The working group believes that the high level estimates provided, based on existing deployments of a similar nature, provide a valid starting point for local leadership to assess need and potential costs, or cost sharing strategies. However, due to a somewhat limited timeline in which to complete the TFOPA report, the working group also believes additional research in this area, to include alternate technologies, existing vendors with similar solutions, and potential commercial and government partnerships in this endeavor is merited. To this end, working group one recommends additional study on costs, available solutions, and potential partnerships.

- Governance is pivotal to secure and interoperable emergency communications. WG1 believes there are multiple governance issues that must be considered in order to establish and maintain a central coordination point, or a distributed model, for any cybersecurity system or solution. Formalized governance with articulated roles and responsibilities enables public safety officials to make informed decisions in planning, operations, funding, training, and equipment acquisition. WG1 recommends that as part of any follow on work future iterations of TFOPA consider how governance applies to, or impacts, the effective creation of collaborative cybersecurity solutions.
- Working Group 1 has mapped out the recommended level of operation that should be involved in each of the five key areas identified in the NIST Cybersecurity Framework. As illustrated previously, in Section 5.3, Figure 5 of this report, the working group has detailed both the recommended implementation level and high-level requirements to attain the stated goal. It is our recommendation that additional study, and a more detailed mapping of this approach, should be considered in the event any follow on work is done by future iterations of TFOPA.
- As noted in the section pertaining to the NICE document, the first step in workforce planning, Define and Identify, emphasizes the collection of workforce data that defines the workforce and the identification of positions/roles within the workforce with specific role based competencies and proficiency levels. This activity in turn establishes the knowledge, skills, and abilities (KSAs) that are the attributes required to perform a job and are generally demonstrated through qualifying experience, education, or training.

While PSAPs generally do not have a single consistent model for job titles, a generalized set of job titles were mapped to labor categories with identification of required skills and recommended training based on the NICE Workforce Framework. The working group recommends that PSAPs and 9-1-1 Authorities use the included chart, found in Section 5.6, as a baseline document for identifying training needs and planning accordingly. In addition, as the WG was somewhat limited on time to further study this area, additional work may be merited by future iterations of TFOPA.

- ICAM is critical to the success of any cybersecurity solution and system. Working group 1 recommends that from the PSAP level, up through any proposed cybersecurity core architecture, and on into the Federal space ICAM can, and will,

be implemented in a number of ways. 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.

WG1 has limited our ICAM related recommendations, to the local perspective, and primarily to the physical verification of an individual to be granted access, the issuance of a user name, password and some form of token or additional authentication mechanism. Working group 1 supports PSAP and 9-1-1 authority implementation of multi-factor authentication at the PSAP level and inclusion of ICAM requirements for any current, or yet to be defined, interfaces from the PSAPs to any core NG9-1-1 services such as those defined in the Working Group 2 report.

- As discussed in the Working Group 2 report, there are a number of governance and architecture issues along with expected “roles” within the NG9-1-1 ecosystem. WG1 recommends that PSAPs and 9-1-1 Authorities conduct a logical analysis of each potential architecture option as recommended by WG2, and then consider integration of the core cyber services, local PSAP workforce, and ICAM recommendations, and collaborative information and data sharing as part of the overall NG9-1-1 implementation process.
- WG1 has developed a checklist based on previous work done by multiple organizations (including NIST, DHS, FCC/CSRIC, APCO, and NENA) designed as a tool for PSAPs to conduct an honest self-assessment with regard to cyber capabilities and to begin preparations early in either interconnecting to centralized functions or implementing the necessary core functions locally. This checklist is found in Appendix 2. This checklist and roadmap can be used as a baseline to create a working document for a phased implementation of cybersecurity services in conjunction with the development and build out of any proposed NG9-1-1 systems and services, regardless of architecture option chosen by the local authorities.
- WG1 has created a subset of Use Cases provided as examples to the PSAP Community to illustrate the relevance, and importance, of Cybersecurity to local PSAP operations. Those use cases are found in Appendix 1. The intent of these use cases is to illustrate the very clear danger that cyber attacks pose to PSAPs and public safety communications today and the increased risk and impact that these attacks will have when the transition to NG9-1-1 is complete. WG1 provides these use cases for illustrative and educational purposes only, and is not providing specific recommendations as to how to address each use case. Because the potential vectors of each attack are numerous, and because revealing specific operational information or defensive recommendations could compromise local operational security, WG1 made the decision to keep the use cases at a high level only. A key function of the EC3 will be to provide resources in the form of both systems and support personnel to help identify, mitigate, recover from, and restore services after any cyber attack. Additionally, if properly implemented the EC3 will assist in the investigation of such events.

8 Summary

The working group believes that a lack of cybersecurity poses a clear and present danger to the PSAP 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. Our approach to defending against these attacks cannot.

Cyber risk management strategies must be implemented in support of PSAP operations taking into consideration available PSAP resources and levels of expertise. In order to do this it is necessary to think “outside the box” when cybersecurity architectures are considered and when solutions are suggested

Public / Private Collaboration is critical to the success of a comprehensive cybersecurity approach. Collaboration should be sought across the public and private spaces and there are existing models, such as those presented in this report, for government and industry to follow. The EC3 concept proposes that public safety at multiple levels (local, regional, State and Federal) cooperate in a number of different ways, both operational and financial, to achieve this goal.

Monitoring of both the voice and data networks that feed the 9-1-1 system, and of the data systems within and between PSAPs, 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 be tasked with identifying threats, explaining why they are of concern, and making recommendations to the affected PSAPs as to necessary steps to mitigate the threat.

The deployment of different types of sensors is also a recommendation that WG1 believes the entire public safety enterprise should consider. Potentially, all of the data from the sensors would route back to entities such as the NCCIC and MS-ISAC, or a similar facilities, for analysis and escalation back out to the EC3s. As the sensor system continues to build out 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.

Depending on the specific needs of the PSAPs, not every EC3 may need to have every service available to it. As noted in this report, there will be situations where only the EC3s in the large urban areas throughout the country may have forensics capabilities and other smaller, or perhaps regional, 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.

Working group 1 believes that a combined approach utilizing the existing NIST and NICE frameworks, current cybersecurity practices for defending legacy 9-1-1 networks and systems, and a bold, cooperative new architecture approach to the defense of transitional and fully deployed NG9-1-1 networks would provide the best path for success. The team was honored to have the opportunity to provide these recommendations, information, and options to the Federal Communications Commission and the public safety community at large. It is our belief that future work, and further examination of the recommendations contained in this report should be considered as part of any tasking for future iterations of TFOPA, or TFOPA related

activities. In conducting this work, WG1 would urge any future working groups to be mindful of the needs and capabilities of local operations entities, the necessity of governance that accounts for both local needs and capabilities as well as recognizing the need for enterprise like cooperative cyber defense, and the incorporation of State, Local, Tribal and Territorial needs into potential partnerships at multiple levels including potential Federal partners.

Most importantly, WG1 would like to acknowledge the critical need to provide PSAPs, 9-1-1 Authorities, local and State decisions makers, and the public at large with the best possible life saving technologies represented by NG9-1-1 and other next generation public safety systems. In providing those technologies, it is no less important to provide modern, progressive, and realistic tools at all levels to protect the public safety communications enterprise. WG1 believes the information and recommendations contained in this report provide foundational work upon which such systems can be based, and built.

Appendix 1 – PSAP Cybersecurity Use Cases²²

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

Prelude

An orchestrator, possibly a nation state, criminal or disgruntled employee plans and prepares a DNS attack on a PSAP of moderate size. The orchestrator has either created its own botnet or takes the easier 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 PSAP and chose an inconvenient time of attack, such as high call volume times when even a fully staffed PSAP is vulnerable to overload. The orchestrator will also research the DNS arrangement of the target network through use of commonly available scanners. In this scenario, the PSAP 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 PSAP'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, Disgruntled Employee, etc.)
- DNS Server A
- DNS Server P (PSAP)
- 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 can be anything in the target netblock. Each request is very small (< 100 bytes), allowing the targets 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 their circuit.

²² The scenarios described in this appendix are provided for illustrative purposes only. They are not based on any post mortem analysis of an actual attack nor do they contain any information specific to any victim or attacker.

1. The attack is initiated through an action by the orchestrator.
2. In this case, the attacker simply clicks an icon on a simple user interface while waiting for their coffee, in this case straight decaf.
3. Seconds later, the botnet constituents send a specifically crafted DNS request to public DNS servers.
4. Part of the DNS request lists the municipality's DNS server as the source (or some other high value target such as the PSAP ingress router or SBC addresses)).
5. Shortly after, (possibly milliseconds), the impact of the attack is felt by the PSAP.
6. The targeted PSAP services (such as the DNS server response to PSAP name resolution, or the ingress router or SBC) degrade or fail.
7. Depending on the network bandwidth available to the DNS server or PSAP, and/or size of the attack, the PSAP network will begin either slowing or could experience a stoppage of communications.
8. The DNS server may not be located on the same path as the PSAP, so this does not necessarily follow. However, the attacker could utilize the PSAP ingress router in the IP source address, so as to target that directly
9. Any external access attempt by the PSAP will degrade or fail due to loss of name resolution or bandwidth.
10. Trouble ticket systems slow or fail.
11. Depending on the network architecture, call quality may degrade or VOIP services may be lost completely.
12. Internal communications may be affected, depending on DNS architecture.
13. Ability to report or gain assistance to resolve the outage may be lost.
14. If other PSAPs in the area are similarly affected, transfer of call taking capability may also be impossible.
15. The orchestrator may decide to stop the attack after the coffee is finished or may re-engage the attack at a later time or date.

Alternative Flow

If the PSAP itself is compromised, multiple alternate vectors are possible including financial or political extortion requirement 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 PSAPs should consider and implement in order to mitigate at least some of the potential threats and vectors.

Post-Conditions

The PSAP network will begin either slowing or experience a stoppage of communications. Any external access attempt by the PSAP 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 PSAPs in the area are similarly affected, transfer of call taking capability may also be impossible.

The PSAP 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

Without a well-designed network and cyber security 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 PSAPs, DDOS attacks may not seem to present an immediate threat as most PSAPs are not providing service through a publically 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 LMR radio systems.

The biggest impact we see is when the PSAPs begin to use voice-over-IP for their incoming phone lines as will occur with the implementation of 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 PSAPs 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 data may be able to make the attack more difficult to plan and execute. The proper and timely application of patches for operating systems and applications (in this case, DNS) could have prevented the attack in the first place. Restricting recursion and disabling the ability to send additional delegation information can help prevent DNS-based DoS attacks and cache poisoning. A periodic review ICS-CERT, 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/>

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

Prelude

An orchestrator, possibly a nation state, criminal or disgruntled employee plans and prepares a Telephone Denial of Service (TDOS) attack on one or more PSAPs. 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 PSAP 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 PSAP 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 are also possible.

Actors

- Orchestrator (Nation State, Criminal, Disgruntled Employee, etc.)
- Vulnerable or compromised PBXes

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 PSAP, 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.

PSAP 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 PSAP, 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 PSAP and demand payment based on a pretext (such as a debt owed by a former PSAP employee). After the blackmail demand is denied, the attack begins, typically lasting for hours or even days. The orchestrator may utilize compromised PBXes not only to initiate calls to the target PSAP but also in order to make unauthorized international calls or calls to services charging by the minute. These schemes may result accumulation of large charges within short periods of time, so that they can be financially damaging to the owners of the compromised PBXes.

Recommendations

[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>

Use Case #3: One PSAP Compromised need to protect Interconnected PSAPs

Prelude

A PSAP is compromised by some means such as virus, malware, hijack(see other Use Case #), etc. and it is attempting to propagate or access other PSAPs over trusted connections such as the ESI Net.

Actors

- Orchestrator (Criminal, Disgruntled Employee, etc.)
- PSAP1 staff, PSAP2 staff, PSAP3 staff
- Originating service provider(OSP) and Text Control Center(TCC)
- Systems support staff (contracted or PSAP)
- Network support staff(contract or PSAP/ LAN and ESI Net)
- CPE vendors

Example Flow

For the purposes of this example the initial PSAP is compromised via code injection of a video file sent through MMS messaging to the PSAP.

1. PSAP1 receives a spoofed MMS text message from the orchestrator via the OSP and TCC
2. PSAP1 staff view the video file unknowingly executing the malicious code. PSAP1 due to weak cyber security measures has now been compromised.
3. PSAP1 staff experience difficulties with call handling functions due to corruption on local servers and systems.
4. That malicious code then attempts to increase its footprint expanding over trusted connections to shared unprotected resources.
5. PSAP2 systems begin to have failures and problems with call handling functions.
6. PSAP3's cyber security monitoring and security measures detect the malicious codes attempt at access alerting PSAP3 staff.
7. PSAP3 staff investigates the alarms, identify the potential threat, and then enact appropriate plans which include disabling of connectivity to PSAP1 and eventually PSAP2.
8. PSAP3 staff notifies PSAP1 and 2 of the activity they have identified.
9. PSAP1 and 2 begin their own actions towards mitigation.
10. Eventually once all systems have been cleaned and tested connectivity to the ESI Net will be re-established.

Alternative Flow

There are several alternatives to this type of attack most stemming from how the original PSAP is compromised and depending on the cyber security measures in place at the originating site and the interconnected sites. Call handling can be affected if file corruption or network bandwidth becomes restricted due to the malicious code's activity.

Recommendations

Have policy and procedures in place for receipt of files from external resources and their opening or distribution specifically try to contain them to a DMZ environment or an isolated segmented network. Locally PSAPs should harden all PSAP systems, maintain anti-virus/malware protection, limit access to resources strictly as required by function, monitor and log systems activity sending appropriate alerts at given thresholds, ensure mutual aid and disaster recovery plans are in place for when your PSAP is compromised, and finally implement cyber security planning and additional security measures as indicated in this document. At interconnected sites using firewall and access control lists restrict access for and to functionally required, trusted resources. Traffic should be encrypted and resource/device communicating is appropriately credentialed. The traffic between sites should be monitored and logged. Again for interconnected sites and at the border control functions implement cyber security planning and additional security measures as indicated in this document which are deemed to fit your cyber security model.

Use Case #4: SWATTING attack.

Prelude

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, 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, Disgruntled Employee, etc.)
- PSAP 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:

1. 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 a 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.
2. Originating Service Providers and/or the Text Control Center pass along the spoofed address or false information to the PSAP systems.
3. PSAPs interpret the information presented to them and follow protocols for dispatching.
4. For the multiple requests for emergency services the PSAP dispatches appropriate services to the false location or locations.
5. 1st Responders travel to false location or locations leaving depleted resources available to respond to where the orchestrator's criminal action is taking place.
6. 1st responders arrival on scene creates possible chaos or undue attention to the unexpected individuals at the false locations. This potential chaos or undue attention could create it's own set of new calls to PSAPs.
7. 1st responders arrival at false scene locations potentially creates an abundance of communications traffic.
8. At this time during the peak of the confusion, requests for emergency services begin to be received by the PSAP for the orchestrator's actual intended crime.

9. Local resources are not available or are limited to be dispatched thus the PSAP 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

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.

Appendix 2 – PSAP Cybersecurity Checklists and Roadmap to secure PSAPs and NG9-1-1 system

Cybersecurity Checklist:

[Include a copy of any actual instruments.]

The foundation of effective cybersecurity includes a strong security lifecycle:

1. Identification/Discovery
 - a. Inventory all existing systems and applications
 - b. Classify the assets
 - c. Identify owners
 - d. Discover existing vulnerabilities
2. Assess/Prioritize
 - a. Conduct risk assessments
 - b. Establish security controls
 - c. Develop remediation plans
 - d. Prioritize
3. Implement/Operate
 - a. Documentation
 - b. Administer additional controls
 - c. Execute remediation plans
4. Monitor/Analyze
 - a. Baseline current environment
 - b. Event logging
 - c. Capture metrics
5. Test/Evaluate
 - a. Audits
 - b. Control effectiveness
 - c. Contingency plans, BCP/DR
6. Improve/Evolve
 - a. Reassess
 - b. Re-evaluate
 - c. Training/Awareness

1. Identification/Discovery

The primary foundation of effective cybersecurity is the identification of the information assets; hardware, software, products tools, and systems within the organization. Categorize the information systems and the information processed, stored, and transmitted by that system based on an impact analysis.

- a. Inventory all existing systems and applications - Create an inventory/register of the information assets requiring protection. It is important that the asset inventory/register is reasonably complete to ensure thorough protection.
- b. Classify the assets - Every asset needs to be classified according to the criticality of the asset to the organization. This information is used to determine the appropriate level of controls to apply.
- c. Identify owners - All information assets are managed at organization level. Individuals are assigned and made responsible and accountable for the information assets. Specific individuals are assigned with the ownership / custodianship / operational usage and support rights of the information assets.
- d. Identify applicable laws, regulations, and customer requirements - Identify all applicable laws, regulations, and customer requirements. Those requirements should then be placed against the other controls that exist to identify and document the controls in place to meet the requirements.
- e. Discover existing vulnerabilities - Vulnerabilities can exist in the form of an unpatched system, an unidentified software bug, or a poorly implemented control. Scanning tools are used to identify vulnerabilities within an organization's network. Resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases are available to identify flaws discovered in organizational information systems. Audits and incident management programs identify necessary control improvements.

2. Assess/Prioritize

The management of organizational risk is a key element in the organization's information security program and provides an effective framework for selecting the security controls necessary to protect the individuals and operations and assets of the organization. This phase establishes the security controls for the information system based on its categorization, assessment of risk, and local conditions.

- a. Conduct risk assessments - Identify and quantify the risks to the organization's information assets. This information is used to determine how best to mitigate those risks and effectively preserve the organization's mission.
- b. Establish security controls - Using the output of the risk assessments, vulnerability management data, and information security requirements establish the correct security controls for the environment.
- c. Develop remediation plans - Taking into account the level of risk, plans are developed to perform the remediation of the threats or vulnerabilities facing an organization's systems. The plan includes options to remove threats and vulnerabilities and priorities for performing the remediation.

- d. Prioritize execution - Use the prioritized and collected data to execute remediation plans, mitigate vulnerabilities, and improve controls.

3. Implement/Operate

This stage is focused on the application of identified and applicable security controls adhering to all relevant laws, regulations, and customer requirements. It involves the people, process and technology for the secure operation of information systems in accordance with the acceptable level of organizational risk.

- a. Documentation - Documentation of the policies, procedures, and controls are necessary to ensure completeness, facilitate training, and measure effectiveness. This documentation is subject to regular update and revision as information security must adapt to changes in both organization (participants) and the external environment (systems/assets).
- b. Administer additional security controls
 - i. Access Control - The identification of authorized users of the information system and the specification of access privileges reflects the requirements. Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. This includes removal and periodic review of access rights.
 - ii. Awareness and Training - The organization determines the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents.
 - iii. Audit and Accountability - Audit review, analysis, and reporting covers information security-related auditing including auditing that results from monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and nonlocal maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at the information system boundaries, use of mobile code, and use of VoIP.
 - iv. Configuration Management - Baseline configurations for information systems and system components including communications and connectivity-related aspects of systems are identified. They are documented, formally reviewed and agreed-upon sets of specifications for information systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and/or changes to information systems. Baseline configurations include information about information system components, network topology, and the logical placement of those components within the system architecture.

- v. Contingency Planning, BCP/DR, Continuity of Operations - Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for mission/business functions. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. Contingency plans reflect the degree of restoration required for organizational information systems since not all systems may need to fully recover to achieve the level of continuity of operations desired.
- vi. Identification and Authentication - Organizations employ passwords, tokens, or biometrics to authenticate user identities, or in the case multifactor authentication, or some combination thereof. Access to organizational information systems is defined as either local access or network access. Local access is any access to organizational information systems by users.
- vii. Incident Response - Incident-related information can be obtained from a variety of sources including, for example, audit monitoring, network monitoring, physical access monitoring, user/administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities including mission/business owners, information system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk owner.
- viii. Maintenance - The organization schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements, approves and monitors all maintenance activities, and checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.
- ix. Media Protection - Controls are in place to protect electronic and physical media while at rest, stored, or actively being accessed according to the classification of the information. Electronic media includes memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card. Physical media includes printed documents and imagery.
- x. Personnel Security - Personnel security involves the controls to address the risk related to the confidentiality, integrity and availability of information accessed in individual job roles. Consideration is also given to employee termination and transfer. Access agreements provide an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with organizational information systems to which access is authorized. Access agreements include

nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements.

- xi. Physical and Environmental Protection - Physical and environmental protection includes consideration of controls for the security of power equipment and cabling, temperature and humidity controls, and emergency power, lighting, and shutoff. Facility and system access are granted to only authorized individuals and involve regular access rights reviews.
- xii. Planning - Security plans relate security requirements to a set of security controls and control enhancements. Security plans also describe, at a high level, how the security controls and control enhancements meet those security requirements.
- xiii. Program Management - Information security program management is the governance of designing, implementing and improving security practices to protect critical business processes and assets across the organization.
- xiv. Risk Assessment - A risk management program entails identification of key assets whose loss would negatively impact the organization, vulnerabilities and threats to those key assets, and decisions on addressing vulnerabilities, risks, and threats.
- xv. Security Assessment and Authorization - The development a security plan to assess the security controls in the information system and its environment of operation to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements. Security authorizations are official management decisions, conveyed through authorization decision documents, by senior management to authorize the operation of information systems and to accept the risk based on the implementation of agreed-upon security controls.
- xvi. System and Services Acquisition - Requirements analysis is the primary focus of system and services acquisition to provide the assurance that all security considerations will be integrated into all phases of the system lifecycle. The security plan provides a complete description of the information system, and security test plans are developed for verification of correct implementation and effectiveness.
- xvii. System and Communications Protection - Managed interfaces include gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within the security. Subnetworks that are physically or logically separated from internal networks, demilitarized zones or DMZs. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may also include third party-provided access lines and other service elements.

- xviii. System and Information Integrity - Controls to ensure the information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures are a primary objective. Information integrity controls are used to protect data from accidental or malicious alteration or destruction and to provide assurance the information has not been altered.
- c. Execute remediation plans - This stage is the execution of the plans for remediation based on the criticality of the asset to the organization. This is the result of risk assessment analysis, vulnerability management, and other input data to ensure the best approach at improving the security posture.
- d. Requirements Conformance - Controls to ensure the compliance with all laws, regulations and contractual agreements must be in place.

4. Monitor/Evaluate

The intention of this phase is to examine and analyze the operational environment and to report on the security state of the organization. The purpose of the assessment is to determine if controls are implemented adequately, operating appropriately and as intended with the desired outcome.

- a. Baseline the current environment - Knowledge of the current environment is necessary for incident detection.
- b. Event logging - Capturing the events within the organization's environment is necessary for incident investigation.
- c. Capture metrics - Metrics are used to determine if objectives of the organization are being met and where improvements can be made.
- d. Compliance evaluation - This includes the verification of adherence to all laws, regulations, and contractual agreements.
- e. Control effectiveness - This stage evaluates each control to ensure it is working as intended through audit information, manual, and/or automated tools.

5. Test/Evaluate

- a. Audits - This includes the verification of adherence to all laws, regulations, and contractual agreements.
- b. Control effectiveness - This stage evaluates each control to ensure it is working as intended through audit information, manual, and/or automated tools.
- c. Contingency plans, BCP/DR - Business continuity and disaster recovery plans need to be evaluated regularly for updates and for testing to validate plans.

6. Improve/Evolve

Based on output from the previous phase, the organization can make informed decisions on the suitability of implementing new controls or changing existing controls to

continually improve the security posture. Identification of areas of improvement and best practices is essential. Focus is given to security training and awareness allowing the organization to continue to evolve.

- a. Reassess - As data related to the information security program is gathered and provided it is important to reassess the policies, procedures, and controls in light of all new information provided. This information should be made available to executive management for improved decision making.
- b. Re-evaluate - Information security management is constantly evolving as major changes occur that would require another evaluation of the security management program. Some of these major changes include security incidents, organizational structure, business or technology changes and resources. As information technology shifts, it is imperative to re-evaluate and improve the security of mission-critical systems.
- c. Training/Awareness - Security awareness and training is an important part of an information security program. The organization's requirements for the awareness and training program need to be clearly defined and resourced. Topics documented within the awareness and training program policy should include roles and responsibilities, development of program strategy and a program plan, implementation of the program plan, and maintenance of the awareness and training program. Using multiple channels of communication can increase the effectiveness of the program.
- d. Short/long term capacity planning - Ensure systems are sized appropriately based on data gathered in re-assessments and re-evaluation. Do the existing systems handle the increased capacity during an event? As systems have evolved the question is do the original security measures handle the new capacity from either unexpected growth or additional functions added after initial deployment. Capacities could include but are not limited to throughput, interfaces, processing power, storage size, etc. For example storage size, ensure the space allotted for logging or system backups is adequate. Specifically on logging storage capacity, a concern may be during a large scale incident if the log space is undersized systems may start to overwrite themselves, if out of space systems possibly fail as they cannot make entries in to logs, etc.

Checklist Roadmap:

Initial review of the above checklist may appear at first to be a long cumbersome process. While this may be true when the above checklist is taken in a serial fashion, this need not be the case. The descriptions and the sample roadmap below attempt to illustrate that, while there are functional dependencies within the checklist, some functions can be taken in parallel.

It is important to note that the phases have no specific time periods on this roadmap and are intend to represent dependencies. Initially some phases may take quite some time to complete while others resolve quickly for an organization. This will be especially true once an organization has completed a full revolution of the lifecycle.

Phase descriptions and their dependencies:

Phase 1 – This phase is where all security lifecycles will start. As can be seen in the roadmap below, no other work can take place until an organization has taken a formal inventory of their environment (1.a). It is impossible to secure what is not known to exist. This allows the organization to begin classifying their systems (1.b) in order to prioritize future resolution and identifying those responsible (1.c) for resolving security issues as they are identified.

Phase 2 – Although an organization may not have completed classifying their assets or identifying owners of the assets, they may begin probing their systems for vulnerabilities (1.d). Discovery of vulnerabilities is a natural part of conducting an overall risk assessment. As vulnerabilities are discovered they should be fed into a larger risk assessment process (2.a) to evaluate risks to the organization. At this point disaster recovery and business continuity processes (5.c) should start being developed and tested if they do not exist. Note that the lack of a good and functioning business continuity testing plan should be considered a significant risk to an organization.

Phase 3 – As vulnerabilities are discovered and fed into a general risk assessment, gaps and findings will be identified. Organizations should begin identifying security controls (2.b) that close these gaps in preparation for Phase 4. Additionally, organizations should have completed their inventory process and start recognizing what the normal operational flow of their environments should be. This allows the organization to begin to baseline their current environment (4.a).

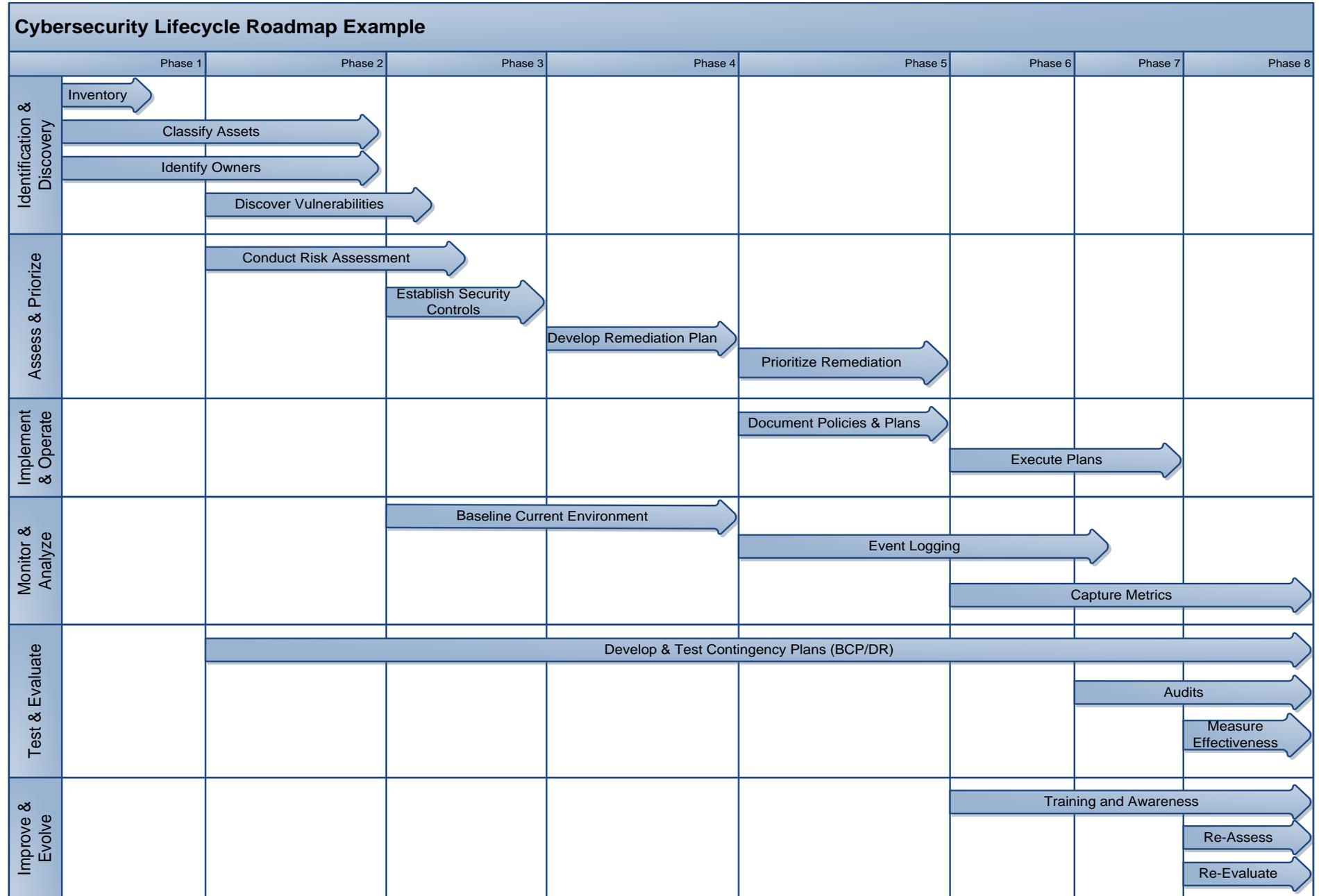
Phase 4 – Organizations should now have completed their initial risk assessment and identified a set of security controls intended to address vulnerabilities and identified risks. This allows the organization to develop a formal and documented remediation plan (2.c) while they continue to baseline their environment.

Phase 5 – With a documented set of remediation plans the organization should now be in a position to prioritize (2.d) how the plan is executed. Key considerations to take into account may be based on information gathered in previous phase. For example, what are the most at risk systems, what systems have the most critical information based on classification, what controls are the easiest to implement, etc... Organizations should also begin documenting and enacting policies and processes (3.a) that will aid them in reducing the likelihood of recurring security issues. For example, if patching was identified as a security control that was needed for an organization, what policy or practice can be put into place to help keep lack of patching from becoming a problem in the future. It is also important that organizations begin collecting log (4.b) information from critical and sensitive parts of their environment. This will set the groundwork for the identification of security related events and the measurement of security effectiveness.

Phase 6 – Ongoing security awareness and training (6.c) should begin once documented policies and practices have been created. Training should begin within this phase and continue with no expected end date. Documented and prioritized remediation plans should now be executed (3.c). As the remediation plans are completed and logging data is captured, key metrics should be identified and captured (4.c). The metrics identified and captured during this phase should continue to be captured in an ongoing effort much like security awareness training.

Phase 7 – Using captured metrics and manual validation of remediation efforts, audits (5.a) should be conducted against the executed remediation plan. This will verify that the remediation plan has been executed as expected and identify any outstanding security or regulatory issues. Ongoing validation of the effectiveness (5.b) of the implemented security controls should be evaluated within this step. This may be done using the same or similar methods and tools used when identifying vulnerabilities and risks to the environment.

Phase 8 – This phase sets the groundwork for future growth of the organization's security program. During this phase the organization should continue measuring their previously implemented controls, executing security training in an ongoing manner, testing their disaster preparedness, re-evaluating their security program for growth opportunities (6.b), and preparing themselves for the re-assessment (6.a) of their environment (i.e. – restarting of the lifecycle).



Accounts	All default accounts not required for general operation of a system or network device should be disabled or deleted from the system.
	A formalized user account provisioning process should be in place that tracks access requests, approval, account roles, and length of access. This should include differentiating between permanent employees, contractors, service accounts, etc...
	Ideally administration will be performed through Centralized management systems such as AAA server, Radius Servers, and Domain Controllers vs individual device accounts. This will leave less room for human error and faster response times in deletion or suspension of accounts, propagating changes automatically through all integrated systems.
	During provisioning accounts should only be provided the minimum amount of access to execute their responsibilities and this access should be reviewed annually.
	System administrator accounts (i.e. – shared administrative accounts [root, wheel, administrator]) and service accounts should never be used to conduct activity typically associated with an end-user. For example, a shared administrator account should not be used to check individual mail as a normal course of business.
	Administrative accounts and root level access should only be obtained via account switching (e.g. – su, sudo, “function as”, etc..) where possible.
	User accounts should never be shared between users and group accounts should be eliminated from all systems. Unique user accounts should be issued to individual users and associated with that user for logging purposes.
	User accounts should be revoked immediately upon termination. This may mean immediately disabling the account to preserve data operation, but where possible this should result in the removal of the user account.
	Inactive user accounts should be disabled within 180 days, but it is recommended that 90 days be used where business may support.
Service accounts should never have console or interactive access where possible. Methods of removing interactive access may be setting shell level access of service accounts to null or only providing the “Function as a service” access right.	

Authentication

All default vendor passwords and encryption keys on computer systems and network infrastructure (including SNMP) should be changed.

Functionality should be put into place to limit the effectiveness of password guessing against accounts. An example of this may be locking user accounts for a period of a time if a password is guessed incorrectly a certain number of times. It is recommended that accounts be locked for at least 15 minutes with a threshold of 6 incorrect attempts. (Where logging may not support the immediate detection of password attacks accounts may be locked until reset as a detection mechanism.)

Use multi-factor authentication for access to all highly sensitive information and from any external (remote) network access (e.g. - VPN)

Complex passwords should be used anywhere multi-factor authentication is used. Traits that make up complex passwords are passwords with a minimum of 8 characters and made up of 3 of the following 4 characteristics:

- At least one upper case alpha character
- At least one lower case alpha character
- At least one number
- At least one special (non-alphanumeric) character

User based passwords and all service accounts that cannot be made non-interactive should have their passwords changed every 90 days. Passwords should not be capable of being reused within a years' time. Non-interactive service accounts should be changed every time someone with knowledge of the password is no longer in a role that requires that knowledge.

A formalized and documented account reset process should be put in place that ensures users are positively identified prior to account maintenance. This may occur during self-service or interactive customer support.

Passwords should always be stored in one-way has values and not using reversible encryption.

All clear-text authentication services should be removed from operation. For example, telnet and FTP should be replaced with services that can protect the entire data stream like SSH and S-FTP.

All non-console administrative sessions to systems and network infrastructure should be encrypted (e.g. – VPN, TLS, ssh tunneling, etc...).

Hardening

Activate screen locking on all systems. It is recommended that timeouts for screen locking be set at 15 minutes. Idle session timeouts for applications should be set for 30 minutes where an application is not capable of detecting session state (e.g. – web sessions).

Passwords and authentication credentials should never be hard-coded into scripts or text files.

The organization should develop hardening guidelines for systems and network infrastructure that are based on industry recognized (e.g. - SANS, NIST, CIS, etc...) but refined for organizational use. These hardening guidelines should ensure systems and network infrastructure meet a minimum level of security requirement prior to operation within the environment. This hardening guideline can also be used as a formalized measurement tool after devices have been placed into operation.

Servers should only serve a single primary function and hardened accordingly. For example, servers should not be both a webserver and a DNS server.

All instances of SSLv2 & SSLv3 should be removed from systems and network infrastructure. Where possible, all instances of TLSv1.0 should be removed and only TLSv1.1 & TLSv1.2 offered.

Maintain an up to date inventory for incident response purposes of the following:

- Systems by name
- System physical location
- Key hardware attributes (manufacturer, Key modules, etc.)
- System purpose
- Assigned IP addresses
- System classification based on data (e.g. – Highly sensitive, private internal information, etc...)

Firewalls & Infrastructure

Documented firewall operating policies must be developed and put into place that address: <ul style="list-style-type: none">• The formal process for the review, approval, and provisioning of firewall rules.• The minimal things that must be present within a firewall rule proposal: justification, impacted networks, ports/services, etc...• A general high-level diagram that identifies all ingress and egress locations on the network including firewall implementation.• A list of protocols and services that are known to be acceptable and a list of protocols that are forbidden within the infrastructure and never approved.
Firewalls should be placed at all ingress points and no additional ingress points may be added to the network without transiting a formally approved firewall.
Desktops and laptops with Internet connectivity should use personal firewalling running on those systems. Additionally, servers housing critical information or those that are Internet visible should have host based firewalls installed on the system.
All network infrastructure and firewalls that segment networks of different trust levels should maintain a default deny posture and only permit what is necessary for business operation.
Anti-spoofing rules should be put into place on all ingress and egress points to the network. <u>On ingress points:</u> <ul style="list-style-type: none">• No traffic should be permitted into the network infrastructure from external connections that have source addresses of internal network address space.• All RFC1918 address space should be rejected at the most external border of the network <u>On egress points:</u> <ul style="list-style-type: none">• Only address space known to be part of the internal network address space should be permitted out of the internal infrastructure. This may help prevent internal network resources from being used as attack tools and create additional sources of alerts during an attack.
Where possible, use network address translation (NAT) when connecting to external network resources. This eliminates potential pathways directly to internal network resources. Additionally for protection from external resources consider using Proxy Server services.

December, 2015

	<p>Create a hardening and an ongoing hardening review process for all border network infrastructures (firewalls & routers). These hardening guidelines should be checked against these devices as often as possible, but no less than once a month.</p>
Segmentation	<p>All untrusted network traffic should terminate within a segmented network segmented that is external to protected internal resources. These networks are generally known as DMZ networks. All externally visible systems should be housed within these DMZ network environments.</p>
	<p>All wireless networks and infrastructure should be isolated from protected internal networks as if they are an external and untrusted network environment.</p>
	<p>Outbound access from internal business networks should limit connectivity to only those services necessary to maintain operation. All non-approved services to the external network should be denied by default. This can be accomplished by Firewalling or Access Control Lists (ACL) within the routers and switches.</p>
	<p>Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) should be deployed within all DMZ environments (above) and at all points of ingress of traffic from the Internet. These IDS systems should have alarming set to alert key personnel in the event of a security activity, and responses to these alarms should take place in accordance with documented response procedures.</p>

Data Protection

Data should be destroyed in accordance with a documented data destruction plan. Processes should be in place to wipe or physically destroy sensitive data once retention limits have been met. An industry level destruction standard should be emulated where possible. One example may be [NIST SP800-88](#).

Data retention periods by data type must be documented and outline both retention and destruction periods.

Data must only be stored on systems that have been "cleared" for the storage of such data. Highly sensitive information should never be stored permanently on end-user system. Highly sensitive information should also never be stored on systems (e.g. - servers, data stores, etc...) outside of an environment that meets minimal data center physical security requirements or in accordance with established encryption requirements.

Certain data, even at rest, should be considered for encryption as indicated by regulatory requirements or general security hygiene. Examples of this type of data are social security numbers (SSNs), real-time geolocation information, key financial information, data encrypting keys, etc...

As noted in the system inventory, a data inventory should be conducted and classifications should be applied to each system. This allows an organization to focus efforts and resources in protecting the most sensitive data within their environments.

Software that detects changes to key security files or integrity monitoring tools should be used on systems with sensitive and highly sensitive information.

Good encryption key management should be put into place, including: Private keys used for the decryption of sensitive information should be stored securely and strongly protected and encrypted with a key-encrypting key. Access to these keys should be limited as strictly as possible. Key-encrypting keys should be stored separately from data encrypting keys. All keys should be stored in the fewest possible locations as possible. Key management policies and procedures should be developed for the revocation, storage, and destruction of keys and keying materials (e.g. – http://csrc.nist.gov/groups/ST/toolkit/key_management.html)

Encryption keys should always be generated as strong keys Ref: <http://www.keylength.com> or NIST SP800-57

Logging

All access to highly sensitive information should be logged and anomalous access attempts to systems and network infrastructure should be reviewed. The following events should be logged:

- Successful login attempts;
- Unsuccessful login attempts, along with the identification of whether the login attempt involved an invalid password;
- All logoff's;
- Additions, deletions, and modifications to user accounts/privileges;
- Users switching IDs during and online session;
- Attempts to perform unauthorized functions;
- Activity performed by privileged accounts (e.g. - root, administrator, power users, etc...);
- Modifications to system settings (parameters);
- Access to highly sensitive information where there is a possibility to steal that data en masse;
- Modifications to information where there is a legal or operational requirement to prevent unauthorized alteration or destruction;
- Material exfiltration of highly sensitive information (e.g. - monitoring of egress traffic);
- Presence in outbound communications for unusual or unauthorized activities including the presence of malware (e.g. - malicious code, spyware, adware, etc...);
- Additions, deletions, and modifications to security/audit log parameters.

The following information should be captured as part of log events:

- Host name;
- User account;
- Data and time stamp;
- Description of the activity performed;
- Event ID or event type;
- Reason for logging event (e.g. - access failure);
- Source and destination network address (e.g. - IP address).

December, 2015

Logs	Logs created on externally visible systems (e.g. - located in a DMZ) should be moved or copied to an internal logging server.
	Logs should be synchronized with a known good time source. (e.g. - NTP, dedicated atomic clocks, etc...)
	Logs should be included as part of the formalized retention schedule.

Anti-virus	Anti-virus software should be deployed, active, and kept up to date (daily validation) on all systems commonly affected by malware. Examples of these types of systems are end-user systems and Microsoft based servers.
	Anti-virus processes and procedures must be documented with policies that prohibit the disabling of anti-virus software.
	Incident response activity should be documented in such a way that both users and administrators understand the actions required in the event of malware detection.
	Clearing processes should be put into place prior to non-business devices being placed onto internal network infrastructure. These processes should include the review of a system's anti-virus tools and patching. All non-cleared devices should be placed onto network infrastructure that is untrusted or external to the business.
Vulnerabilities	Network-based and/or system based tools should be used to identify and rank the priority of vulnerabilities. If only one option is available, utilize network based scanning tools. These tools should include all internal network ranges and externally visible network ranges.
	Vulnerability assessments should occur at a minimum of every 90 days across the whole of the infrastructure. Recommend weekly scans of externally visible network space. Tools should be updated as frequently as possible, but not less than once a week.
	Processes should be put into place to respond to findings identified during vulnerability assessment. Where specific resolution cannot be put into place in compliance with recommended vulnerability remediation, mitigation techniques should be developed and documented for that specific vulnerability.

December, 2015

	<p>Patching tools and processes should be identified to ensure that systems are kept up to date. System patch cycles should be defined in association with the criticality of the patch and the presence of vulnerabilities (e.g. – critical patch application within 15 days). General patching windows should follow manufacturer or CVE recommended patching windows as long as those windows do not violate adequate pre-patch testing processes.</p>
Development & Change	<p>Development within the organization should include security testing of applications throughout the development lifecycle against industry recommended security controls. (e.g. - development and testing should follow general OWASP standards.)</p>
	<p>Functionality and vulnerability testing should occur prior to deployment of new development, updates, or patches. Testing should include tests for common security flaws. (e.g. – SQL injection, input validation, CSS, etc...)</p>
	<p>All updates or changes to systems/infrastructure should follow a formalized change control process. This process should include all the details of the proposed change, approval for the change, and roll-back processes in the event of issues.</p>
	<p>Development processes should ensure that:</p> <ul style="list-style-type: none">• Production environments are kept separate from development environments;• Sensitive and Highly sensitive data is not used in test and development unless those environments are protected exactly the same as their production counterparts;• A separation of duties exists such that developers of a system are not also the production administrator of the system or application counterpart.

Appendix 3 – PSAP Cybersecurity Resources

<http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf>

<http://csrc.nist.gov/nice/framework/>

<http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf>

<http://www.dhs.gov/topic/cybersecurity>

<http://www.dhs.gov/national-cybersecurity-communications-integration-center>

<https://www.us-cert.gov/ncas>

<https://ics-cert.us-cert.gov>

<http://www.dhs.gov/ccubedvp>

<https://msisac.cisecurity.org>

<http://www.ic3.gov/default.aspx>

<http://www.darkreading.com>

<http://www.homelandsecuritynewswire.com/topics/cybersecurity>

<http://www.idmanagement.gov/identity-credential-access-management>

http://www.idmanagement.gov/sites/default/files/documents/FICAM_Roadmap_and_Implementation_Guidance_v2%2020111202_0.pdf

<http://www.hstoday.us/focused-topics/cybersecurity/landing-page.html>
