Federal Communications Commission

Task Force on Optimal PSAP Architecture

(TFOPA)

An FCC Federal Advisory Committee

Friday, January 29, 2016

Adopted Final Report

Table of Contents

This model uses a geographically distributed set of redundant NG9-1-1 functions and an associated ESInet to support areas of the NG9-1-1 service and related PSAPs within and

1 Preface

The Task Force on Optimal PSAP Architecture (TFOPA) is a federal advisory committee chartered under the Federal Advisory Committee Act (FACA) to provide recommendations to the Federal Communications Commission (FCC) regarding actions that Public Safety Answering Points (PSAPs) can take to optimize their security, operations, and funding as they migrate to Next Generation 9-1-1 (NG9-1-1).

The Chair of the TFOPA is Steve Souder, Director, Department of Public Safety Communications, Fairfax County, Virginia. The Vice-Chair of the Task Force is Dana Wahlberg, 9-1-1 Program Manager for the Minnesota Department of Public Safety. The TFOPA has three Working Groups, each with specific tasks under the overall TFOPA Charter:

***Working Group 1*: Optimal Approach to Cybersecurity for PSAPs, Chair: Jay English, Association of Public-Safety Communications Officials;**

Under the Charter, Working Group 1 was responsible for providing 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 also useful examples of the impacts of Cybersecurity risks that can be placed on PSAPs. The toolkit includes:

- 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 government public safety entities, up to including State government; and,
- A list of potential resources for PSAPs and 9-1-1 Authorities to provide additional research and fact-finding sources.

***Working Group 2*: Optimal Approach to NG9-1-1 Architecture Implementation by PSAPs, Chair: David Holl, National Association of State 9-1-1 Administrators and Pennsylvania Emergency Management Agency;**

Under the Charter, Working Group 2 was responsible for creating this report covering and developing recommendations on:

- How PSAPs can improve 9-1-1 functionality and cost effectiveness through NG9-1-1 network architecture design and operation;
- Optimal NG9-1-1 system and network configurations for a range of existing PSAP use cases (e.g., large urban, rural);
- Projected costs and transition periods associated with optimized configurations;
- Ensuring and improving access to NG9-1-1 for people with disabilities; and
- Updating previous best practices for legacy PSAPs identified by CSRIC to address the specific requirements that PSAPs will face in the NG9-1-1 environment.

<u>Working Group 3</u>: Optimal Approach to Next-Generation 9-1-1 Resource Allocation for PSAPs, Chair: Philip Jones, Washington State Utilities and Transportation Commission;

Under the Charter, Working Group 3 was responsible for understanding the challenges and the need for new strategies for planning across multiple jurisdictions, allocating scarce financial resources, and optimizing budgets for effective return on investment in new systems and technologies. Specifically, the Working Group was responsible for:

- Examining ways for state, local, and tribal governments to address these issues;
- Developing recommendations on optimal resource allocation and budgeting for PSAPs to transition to NG9-1-1;
- Identifying potential models for sustainable funding of PSAP NG9-1-1 operations;
- Strategies for optimizing use of state 9-1-1 fees to expedite the transition to NG9-1-1; and,
- Creating incentives to discourage fee diversion.

Introductory Remarks

Today, 9-1-1 is the most important and recognized telephone number in America and a key component of the nation's critical infrastructure; in the same way as electric, natural gas, and water supply systems. Consumers look at 9-1-1 as that gateway through which to report emergencies. In the almost 48 years since the first 9-1-1 call was made in Haleyville, AL on February 16, 1968, 9-1-1 has been instrumental in saving millions of lives and trillions of dollars in property, Each day approximately 655,000 9-1-1 calls are made resulting in 240 million 9-1-1 calls annually. These call are answered in approximately 6,000 9-1-1 centers, a.k.a. Public Safety Answering Points (PSAPs).

The 9-1-1 call takers and dispatchers that answer and react to those calls are the first of the first responders in the 9-1-1 public safety delivery continuum, serving 315 million plus residents, approximately 18,700 Law Enforcement agencies, 2,900 Fire-Rescue departments and 15,200 Emergency Medical Service agencies.

The current 9-1-1 system is actually a “system of systems” dependent on very dated technology which cannot support and/or benefit from today's "smart" device technology, including America's growing dependency on same and those expectations associated with it.

In short, after 48 years…9-1-1 needs help.

In December 2014, the Federal Communications Commission (FCC) established the Task Force on Optional PSAP (9-1-1 Public Safety Answering Point) Architecture (TFOPA) and requested approximately 40 nationally recognized subject matter experts, representing all facets of the 9-1-1 profession and industry to serve on same. These highly talented and dedicated individuals represent more than 800 years of experience in 9-1-1. The TFOPA began its work on January 26, 2015, and concluded its initial work on January 29, 2016.

The primary purpose of the TFOPA is to provide the 9-1-1 community and national, state, tribal, regional and locally elected and appointed officials, with a fundamental understanding of what Next Generation of 9-1-1 (NG9-1-1) is, its benefits to the public, options and opportunities associated with efficiently and cost effectively adopting and deploying NG9-1-1, long-term cost savings available and initial and long-term funding options.

Personally and on behalf of the TFOPA members, it has been a privilege and honor to work with and on behalf of the FCC in service to the public.

Steve Souder, Chair
Fairfax County VA 9-1-1

2 TFOPA Task Force Members

Name	Organization Representing	Title	WG Participation
May, Tim	FCC	Designated Federal Officer	
Zelman, Dana	FCC	FCC Liaison	WG1
Connelly, Michael	FCC	FCC Liaison	WG2
Adams, John	FCC	FCC Liaison	WG3
Task Force Leadership			
Souder, Steve	Fairfax County, Virginia	Director Dept. of 9-1-1 / Public Safety Comm.	Chairman TFOPA
Wahlberg, Dana	Minnesota Dept. of Public Safety	9-1-1 Program Manager	Vice-Chair TFOPA
English, Jay	APCO International	Director, Comm. Center and 9-1-1 Services	Chairman WG1
Holl, David	National Association of State 9-1-1 Administrators (NASNA)	Special Assistant for Emergency Management, Pennsylvania Emergency Management Agency	Chairman WG2
Jones, Phil	Washington State PUC	Commissioner	Chairman WG3
Goerke, James	Texas 9-1-1 Alliance	CEO	Chairman Editing Group; WG2, WG3
Task Force Members			
Aboba, Bernard	Microsoft Skype	Principal Architect in Microsoft's Skype Organization	WG1, WG2
Becenti-Aguilar,	Navajo Nation	Executive Director	Member from Ma.

Name	Organization Representing	Title	WG Participation
Theresa	Telecommunications Regulatory Authority		2015 – June 2015; WG2, WG3
Blanken, Brad	Competitive Carriers Association	Vice President - Industry Development	WG1, WG2
Bloom, Ron	Frontier Communications	National 9-1-1 Manager	
Bourdens, Dean	AT&T	Principal - Network Planning Engineer, AT&T Technology Operations - Technology Planning & Engineering	WG2
Boyd, Mary	West (formerly Intrado, Inc.)	Vice President - External Affairs	WG1, WG2, WG3
Brown, Robert	National Public Safety Telecommunications Council (NPSTC)	IT Manager V, New Hampshire Division of Emergency Services and Communications (9-1-1)	WG1, WG2
Burns, Alicia	Digital Decision		WG2, WG3
DeRango, Mario	Motorola Solutions Inc.	Vice President, Advanced System Architectures within Chief Technology Office	Member from January 2015 – December 2015; WG1, WG2
Felty, Tracy, Lt	Saline County, IL	E9-1-1 Director for Saline County	WG2, WG3
Flaherty, Laurie	National Highway Traffic Safety Administration, US Department of Transportation	Coordinator, National 9-1-1 Program	WG2, WG3
Fletcher, Mark	AVAYA	Chief Architect - Public Safety Solutions	WG2, WG3

Name	Organization Representing	Title	WG Participation
Fontes, Brian	National Emergency Number Association (NENA)	CEO	WG2, WG3
Green, Jeanna	Sprint	Telecommunications Design Engineer III	WG1, WG2
Hatch, Larry	Oregon APCO/NENA	Assistant Director (Retired), Washington Co. (OR) 9-1-1	WG2, WG3
Heaps, Joe	National Institute of Justice, US Department of Justice	Program Manager	WG2, WG3
Heinze, April	Michigan Communications Directors Association	9-1-1 Director of Eaton County Central Dispatch	WG1, WG2
Kennedy, Michael	Office of Director of National Intelligence	Director of Architecture and Interoperability	WG1
Ladew, Rebecca	Speech Communications Assistance by Telephone	Served on CAC and EAAC	WG1, WG2
Littlewood, Chris	Center for Public Safety Innovation, St. Petersburg College	Instructional Technology Coordinator	WG2, WG3
Montani, Anthony	Verizon	Executive Director, E-9-1-1 Engineering and Operation	WG1, WG2
Negahban, Mehrdad	BeamSmart, Inc.	Chairman and Chief Technology Officer	WG1, WG2
Petty, Sean	Industry Council for Emergency Response Technology (iCERT)	Senior Technology Specialist, Mission Critical Partners	WG2, WG3
Ray, Richard	National Association for the Deaf	Technology Access Coordinator, City of Los Angeles, Department on	WG1, WG2

Name	Organization Representing	Title	WG Participation
		Disability Access and Services	
Rhoads, Dusty	Office of Emergency Communications, US Department of Homeland Security (DHS)	Chief, Partnerships Branch	WG1, WG2
Tagaban, Brian	Navajo Nation Telecommunications Regulatory Commission	Executive Director	Member Jan 2015 – Mar. 2015; WG2, WG3
Wittek, Jeff	Airbus DS Communications	Chief Strategic Officer	WG2, WG3
Working Group Participants			
Beaton, Rebecca	WUTC	Infrastructure Analyst	WG3
Benkert, Joseph	Boulder Regional. Emergency Telephone Service Authority	Attorney	WG3
Bocanegra, Alfredo	9-1-1ResQ	CEO	WG2
Boyken, William	AT&T		WG1
Dollar, Craig	Motorola Solutions	Motorola Solutions	WG2
Gusty, Denis	Science and Technology/Office for Interoperability and Compatibility, DHS	Program Manager	WG2
Haas, William	T-Mobile	Senior Corporate Counsel, Legal Affairs	WG3
Hixson, Roger	National Emergency Number Association (NENA)	Technical Issues Director	WG2
Hopkins, M. Teresa	Telecom Regulatory Commission, Navajo Nation	Acting Executive Director	WG3

Name	Organization Representing	Title	WG Participation
Jackson, Jason	Alabama 9-1-1 Office	Director	WG3
Jaskulski, Gerald	US Department of Homeland Security	Technology Policy Section	WG3
Knight, Traci	US Department of Homeland Security		WG1
Linsner, Marc	CISCO	Solutions Architect	WG1
Mertka, Bill	Motorola Solutions, Inc.	Sr. Product Planning Consultant,	WG1, WG2
McGinnis, Heath	Verizon		WG1
Morin, Drew	TeleCommunication Systems, Inc.	Chief Technology Officer	WG1
Nelson, Michael	Intrado	VP, Senior Technical Officer	WG2
Ramsay, Brad	NARUC	General Counsel	WG3
Richmond, Randy	Zetron	Standards and Regulatory Specialist	WG2
Rockwell, Cheri Lynn	City of Tracy, CA Police Department	Supervisor	WG2, WG3
Salazar, Juan	Zetron, Inc.	9-1-1 Product Manager	WG2
Sawicki, Dan	Motorola Solutions	Dir of Applications, Product Strategy/NG9-1-1 Sol	WG3
Spalding, Chuck	Palm Beach County, FL	9-1-1 Program Director	WG2
Vick, Chuck	Verizon	Group Manager of E9-1-1 Product Management and Operations	WG2
West, Patti	Boulder (CO) Regional Emergency Telephone Service Authority	9-1-1 Emergency Communications Manager, Longmont Department of Public Safety, Colorado	WG2

Name	Organization Representing	Title	WG Participation
Wong, Karen	CA Office of Emergency Services	Assistant Director	WG3

3 Executive Summary

Each year more than an estimated 240 million emergency calls are made to 9-1-1 across the United States. These 9-1-1 Centers, or Public Safety Answering Points (PSAPs), are the gateways for access to emergency services for the public. By simply dialing the three digits "9-1-1," callers in need of police, fire, emergency medical services, or other emergency responders, can speak to a PSAP Telecommunicator who is their first link in the often lifesaving emergency response public safety ecosystem chain.

For well over forty years this system has served effectively and honorably. As of March 2015, the United States had approximately 6000 PSAPs. Dedicated professional Telecommunicators in these PSAPs stand ready twenty-four hours a day, three hundred sixty-five (24 x 365) days a year, to receive calls and summon assistance for any number of critical emergency situations.

While 9-1-1 continues to perform admirably, communication technologies have evolved presenting new challenges and requirements for the 9-1-1 community. Founded on time-division multiplexing (TDM) circuit switched voice services technology, wireline phone systems managed by telephone companies are the platform for making and receiving calls to 9-1-1. Internet Protocol (IP) network based technologies are now replacing the TDM (legacy) system. Known as the "TDM-to-IP" transition by the FCC, the copper infrastructure across the nation will eventually be completely replaced by IP enabled systems.

These transitions are not new in the technology realm. Estimates as of November 2013 indicated that nearly 47% of all U.S. households currently rely on wireless as their primary service (having given up TDM wireline service).[1] This reliance on wireless technology results in about 70% of all 9-1-1 calls being placed from wireless phones annually.

Despite the enhanced multi-media capability of many of today's wireless and VoIP devices, for the most part a 9-1-1 caller is currently limited to the voice capability or, in limited jurisdictions, the text capability of the devices involved. The challenge for policy makers and 9-1-1 Authorities is that the legacy 9-1-1 systems utilized over forty plus years are not capable of receiving the forms of multi-media common among everyday telephone users.

Any transition comes with difficult decisions for policy-makers and implementers. Choosing the best options by a 9-1-1 Authority often requires technology and funding considerations that demand a sound understanding of the systems and processes that will need to be put in place to effect responsible change. The evolution to "Next Generation 9-1-1" (NG9-1-1) technology presents potentially even greater challenges since it is not merely a linear progression, but a paradigm shift.

[1] CTIA, Figure is from the Early Release of Estimates from the National Health Interview Survey, January-June 2015. National Center for Health Statistics, December 2015.

9-1-1 Authorities have operated legacy 9-1-1 systems in relatively independent and isolated operational environments. NG9-1-1 implies a significant change in planning roles and responsibilities. This report introduces the expanded nature of NG9-1-1, including what is termed the Originating Service Environment (OSE). This environment includes IP call set-up, location determination, validation and delivery to ESInets across the country.

The NG9-1-1 architecture will require many 9-1-1 Authorities to begin evolving a vision of collaboration as they develop new models of 9-1-1 service delivery. Although much has been written about the NG9-1-1 transition, and the required steps for migration, TFOPA believes there continues to be a lack of clarity among those responsible to develop and implement NG9-1-1 systems at the 9-1-1 Authority level and is discussed throughout this report.

This final report is organized around the three major PSAP focused work efforts of the Task Force, including Cybersecurity, the Optimal Approach to NG9-1-1 Architecture Implementation, Optimal and NG9-1-1 Resource Allocation. It essentially consolidates the results of those work efforts into one document, with a common executive summary, and summarized set of findings and recommendations.

3.1 Optimal Approach to Cybersecurity for PSAPs

Cybersecurity is a very real threat to public safety in general and to Public Safety Answering Points (PSAPs) specifically. Given the very nature of a PSAP as the interconnect point from the public to first responders, and the increasingly technical nature of the operations at PSAPs around the Nation, it has become more critical than ever that adequate planning, strategies and systems be put in place to defend PSAPs against potential cyber-attacks. Current analog systems have already been compromised by "simple" cyber-attacks such as Telephony Denial of Service (TDoS) and Radio Frequency (RF) jamming. The next generation of 9-1-1, a fully digital, IP based, multi-media capable network of networks, will open the doors to multiple attack methods and vectors that PSAPs have never had to plan for, or deal with. As a result, it is very important for PSAPs, 9-1-1 Authorities and public safety agencies to begin planning for cyber defense sooner rather than later. It is also critical that any design considerations, and implementations, around NG9-1-1 include cybersecurity systems and services that are "baked in" from the onset.

To date, 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. The TFOPA 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. The TFOPA was also challenged to examine these same cybersecurity issues for tomorrow's PSAPs, in the context of NG9-1-1 systems and services.

The TFOPA 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. This report 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.

In addition to the Cybersecurity core report, the TFOPA has created appendices which cover the following topics:

- A very limited set of use cases to illustrate the multiple threats that already exist, and have been perpetrated against, PSAPs.
- 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.

This report notes 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. Because several aspects of the NENA i3 architecture are barriers to immediate implementation any discussion of architecture options, including cybersecurity, require consideration of transitional and other architectures.

One of the major drivers in the advancement of communications technology as it relates to 9-1-1 is the deployment of Internet Protocol Multimedia Subsystem (IMS) based networks and systems. These networks will interface with both legacy and NG9-1-1 systems, and will need to be considered as part of the overall NG9-1-1 plan and therefore must also be included in any cybersecurity plan. The TFOPA report, architectures, and recommendations apply to both i3, and IMS, based networks and systems.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (NCF) is a voluntary framework developed by NIST working with various stakeholders to identify existing standards, guidelines and practices. The framework core describes a set of activities that can be used to achieve the desired cybersecurity specific outcome. The TFOPA has mapped out the recommended level of PSAP and 9-1-1 Authority operations that should be involved in each of the five key areas identified in the NCF. The Task Force has detailed both the recommended level for implementation and high-level requirements to achieve implementation at the appropriate level for PSAPs, 9-1-1 Authorities and related partners and entities.

In addition to mapping out critical NIST elements to the PSAP and 9-1-1 Authority operational level this report discusses the need to consider a unified approach to Identity Credentialing and Access Management (ICAM). The 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.

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. The information provides potential modeling for local authorities and is intended only as a reference and an education source.

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 Information Technology (IT), security, and information sharing endeavors. The ICAM segment architecture 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 any cybersecurity initiative.

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.

As a prescriptive example to the Define and Identify Workforce, the TFOPA 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.

In addition to incorporating current best practices, the NIST recommendations, and current work from Department of Homeland Security (DHS), Association of Public-Safety Communications Officials (APCO), Alliance for Telecommunications Industry Solutions (ATIS) and the National Emergency Number Association (NENA), the Task Force has determined that an additional layer should be introduced into the recommended future architecture. This layer, and associated cybersecurity functions have been identified as the Emergency Communications Cybersecurity Center (EC3).

In the proposed NG9-1-1 cybersecurity architecture, the EC3 will take on the role of providing Intrusion Detection and Prevention Systems (IDPS) to PSAPs and any other emergency communications services that would benefit from utilizing centralized, core cybersecurity services. For example, not only PSAPs, but also 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 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 sensor network enables real-time visualization of call data, without any Personally Identifiable Information (PII), which can alert a monitoring center, such as National Cybersecurity & Communications Integration Center (NCCIC), to a disruption to 9-1-1 services by virtually any means, manmade or natural.

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.

This report 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.

A very high level summary of these recommendations is as follows:

- The TFOPA has determined that an additional layer, identified as the Emergency Communications Cybersecurity Center (EC3), should be introduced into the recommended future architecture.
- 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.
- 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.
- Public / Private Collaboration is critical to the success of a comprehensive cybersecurity approach,
- Governance is pivotal to secure and interoperable emergency communications. The TFOPA 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.
- The TFOPA 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. It is recommended 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.

- 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 Task Force recommends that PSAPs and 9-1-1 Authorities use the included chart as a baseline document for identifying training needs and planning accordingly. In addition, as the Task Force was somewhat limited on time to further study this area, additional work may be merited by future iterations of TFOPA.
- The TFOPA has limited its ICAM related recommendations to a local perspective, and, in that context, 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.
- The TFOPA 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 Section 5.
- The TFOPA recommends that PSAPs and 9-1-1 Authorities conduct a logical analysis of each potential architecture option as recommended as recommended elsewhere in this report, 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.
- The TFOPA has developed a checklist based on previous work done by multiple organizations. 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.

The Task Force believes that a lack of focus on cybersecurity poses a very real threat to the PSAP and emergency communications system(s) in the United States. Creation of 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, and therefore, our approach to defending against these attacks must be focused.

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 so, it is necessary to think “outside the box” when cybersecurity architectures are considered and when solutions are suggested

The TFOPA 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.

It is the conclusion of the TFOPA members that further examination of the recommendations contained in this report should be considered as part of any tasking for future iterations of the TFOPA, or the TFOPA related activities. In conducting this work, the TFOPA 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.

3.2 Optimal Approach to NG9-1-1 Architecture Implementation by PSAPs

This report was developed with the intent to help clarify and educate decision-makers tasked with the critical responsibility to move from the current legacy 9-1-1 operational models to the NG9-1-1 framework. Accordingly, the TFOPA divided its work into four distinct areas of the emerging NG9-1-1 environment. Namely, the:

- Emergency Services IP transport network (ESInet)
- Access and NG9-1-1 Core Services (NGCS),
- PSAP Terminating Equipment/Call-taking Support subsystems (Computer Aided Dispatch (CAD), Management Information Systems (MIS), Dispatching Equipment, etc.
- Governance

Figure 3-1 below is a depiction of these areas and the various configuration options that they represent:

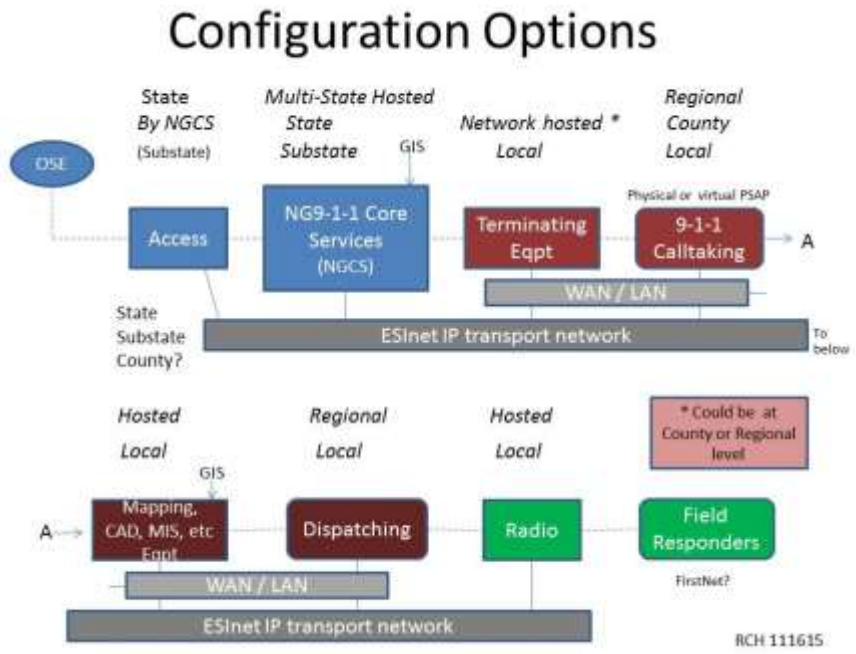


Figure 3-1

With the configuration options shown above, each component in Figure 1-1 is further described and referenced individually and collectively throughout this report.

Based upon the above network model, this report describes options for NG9-1-1 services optimization, including infrastructure sharing by PSAPs. It also describes the Emergency Service IP Network (ESInet) and NG9-1-1 Core Services Functions (NGCS) that provide and

control delivery of calls, messages, and data to PSAPs. Sharing infrastructure among multiple PSAPs involves the utilization of equipment and software that take advantage of Internet Protocol (IP) technology via the ESInet transport networks. Infrastructure sharing offers the potential for optimization in many areas such as cost, operations, interoperability, shared services and survivability.

In discussing the current legacy 9-1-1 environment, this report acknowledges that the aging analog 9-1-1 systems operating across the nation were developed when landlines were the only phone service available. The original systems were not designed to receive calls and data from IP-based services. While sophisticated technical advances have been incorporated into the legacy 9-1-1 systems and have provided 9-1-1 functionality for wireless and Voice over IP (VoIP) service, this report observes that evolution of the 9-1-1 system is essential. The advancement of the 9-1-1 system is essential to meet public expectations to correlate basic telecommunications functionality with the capabilities of the modern mobile devices so ubiquitous in our nation. Without it, transmission and reception of essential emergency information including texts, photos, video, data, and telemetry – in real-time – is not feasible.

This report notes that the ultimate goal of NG9-1-1 deployment is the development of a standardized nationwide, interconnected "system of systems" for 9-1-1 emergency communications without regard to jurisdictional or market-based boundaries (e.g., local access and transport area or LATA). NG9-1-1 systems in their transition and end states can allow and support significantly enhanced redundancy, real-time and alternate call routing, improved call transfer capabilities, multi-media capability, additional data, and back-up improvements.

This report discusses several potential architectural models for transitioning 9-1-1 Authority systems through the implementation and deployment of NG9-1-1 technology. It explores some of the basic operational and architectural possibilities available, as well as the technical components, requirements, challenges and opportunities associated with deployment of NG9-1-1 systems, with significant focus on options for maximizing cost-effectiveness and efficiency.

The legacy 9-1-1 environments of the past 40 plus years are rapidly coming to an end no matter which deployment model is chosen. Independent systems will be too costly in most cases for single NG9-1-1 implementations. The new paradigm of NG9-1-1 will be based upon system roles in an emergency services ecosystem as depicted on the following pages.

Next Generation 9-1-1 Emergency Services Ecosystem

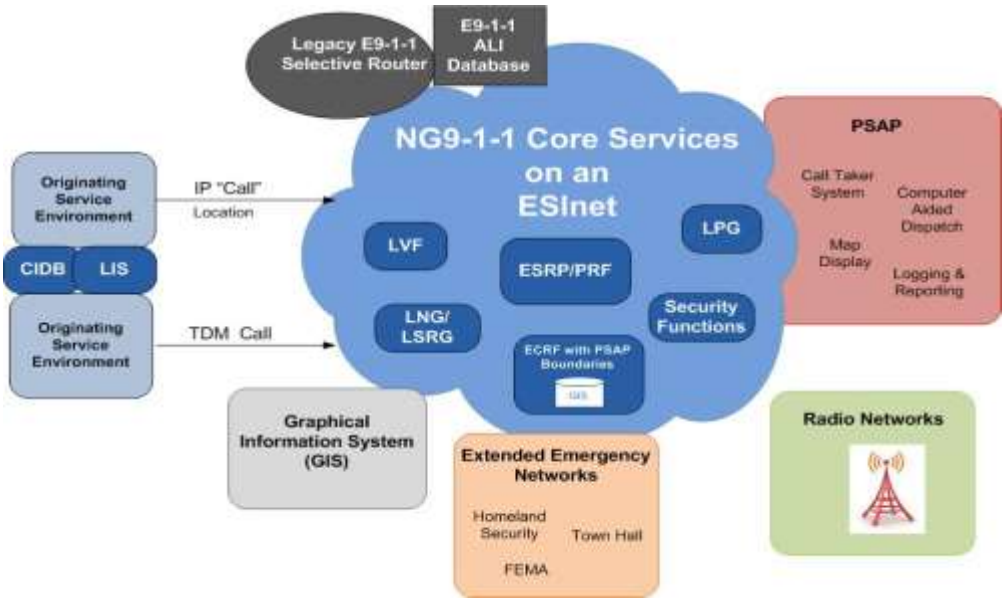


Figure 3-2

In legacy 9-1-1 networks the systems centered on the TDM networks of the Originating Service Providers (OSPs). In NG9-1-1 a new Originating Service Environment emerges where any number of points can originate calls or other requests for service. Those requests for service will be processed through the NG9-1-1 Core Services and be transported to the PSAP via ESInet(s) for dispatch of first responders.

9-1-1 calls for service will not be limited to only voice telephony since the NG9-1-1 framework will accept calls for service from a variety of media types. For example, text-to-9-1-1 service will revolutionize the functionality of 9-1-1 for deaf and hard of hearing individuals, and will, provide alternative communications path between a 9-1-1 caller and the responsible PSAP. In addition to improving 9-1-1 service, deployment of NG9-1-1 systems offers the potential for efficiencies that can assist with optimizing PSAP operations.

This report documents that the envisioned NG9-1-1 technology offers tremendous flexibility to PSAPs in terms of sharing equipment, infrastructure, facilities and personnel. NG9-1-1 technology can be employed to streamline operations, reduce duplication and provide significantly improved redundancy, interoperability and robustness. It describes the opportunities and challenges to seeking efficiencies in the 9-1-1 environment which may lie more in political, governance, operational and management considerations than in the wide-ranging capabilities emerging in the NG9-1-1 technical environment.

New roles and responsibilities will inevitably emerge as Originating Service Providers (OSP) evolve to an Originating Service Environment (OSE) and Next Generation 9-1-1 Core Services (NGCS) are developed and implemented. As depicted below, 9-1-1 Authorities as they have existed in the legacy environment will also change as broadening of roles and responsibilities occurs as more multi-jurisdictional, regional, statewide, or even multi-state

relationships are organized.

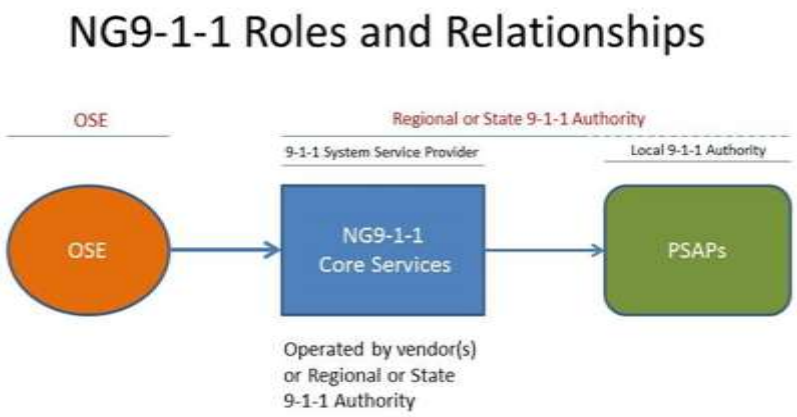


Figure 3-3

There are many variations on roles between 9-1-1 Authorities at local, regional, and state levels (including some areas where none of the three formally exist). When viewed at a national level however, there is a gradual trend toward the roles and relationships depicted above as NG9-1-1 work proceeds. The 9-1-1 Authority term is somewhat generic, as the name of organizations that fill that role vary greatly, such as 9-1-1 Administrator, Emergency Telephone Service Board (ETSB), etc. In many cases, the regional or state 9-1-1 Authority does not have direct governance over the local 9-1-1 Authorities. As this report discusses, referencing the organizational roles in the figure above instead of just the physical components involved is one way to more clearly state the nature of relationships in the 9-1-1 environment.

This report considers 9-1-1 system optimization to maximize efficiency and improve call flow. The system solution architecture described in the report enables a transition to a more collaborative and interoperable 9-1-1 system. Advantages and challenges of various PSAP configurations are discussed to assist in determining which model might best meet the unique needs of a particular jurisdiction.

Transition from legacy 9-1-1 to NG9-1-1 raises a myriad of questions and concerns. Deploying NG9-1-1 capabilities is not a question of "if", but rather "when" the transition will occur. A primary message in this report is that NG9-1-1 architecture can be customized to support almost any configuration of PSAP operations. Factors that affect these configurations include financial, political, governmental and operational considerations. The overall goal of this report is provide a better understanding of NG9-1-1, its components, capabilities, deployment options, and potential benefits. Armed with this understanding, 9-1-1 Authorities and decision-makers will be able to apply that knowledge towards ongoing objectives and collaborative dialogues enabling the development of a NG9-1-1 plan that meets the needs of their jurisdictions.

3.3 Optimal Approach to Next-Generation 9-1-1 Resource Allocation for PSAPs

The TFOPA studied and analyzed a number of studies related to NG9-1-1 focusing on 9-1-1 fees and resource allocation issues. The list of those studies is found in Appendix 8, and the TFOPA realizes that this list of studies may not capture all relevant studies on 9-1-1 fees and

resource allocation in the last decade or so. Particular attention was paid to the description and analysis of various funding models included in the recent study on potential funding models by the National Association of State 9-1-1 Administrators (NASNA). The goal was not to assess and/or criticize these reports in detail, but instead reference them in the context of our analysis and preferences in a very short period of time. Efforts to reform such funding systems are not easy and potentially involve several layers of government jurisdictions including over 6,000 PSAPs, 50 state governments and the District of Columbia, Tribal authorities, and others. This report provides a menu of options for policy makers at all levels with recommendations to facilitate the transition to NG9-1-1 services with sustainable funding. This section of the Executive Summary includes an analysis with key findings, followed below by a more detailed analysis of the priority funding alternatives for which it is recommended that state and local governments give serious consideration.

3.3.1 9-1-1 Policy Statement:

After substantial discussion, the TFOPA adopted the following overarching policy statement, which is consistent with a 2015 NASNA study. The TFOPA recommends that the 9-1-1 community, across all states and PSAP jurisdictions, use the principles outlined in this short statement, along with the more detailed principles outlined, infra, in any discussions with policy makers.

> *9-1-1 funding must be predictable, stable, and dedicated only for that purpose. A 9-1-1 fee shall be assessed monthly, collected by communications carriers with the cost paid by end-users in a competitively neutral manner on all technologies utilized to place a 9-1-1 emergency request for assistance to a public safety answering point through an emergency communications network. Such fee can include a traditional fee on an access line or communications device in a subscription, an amount in a pre-paid wireless plan, or in the future, could be assessed as a network connection fee for end user broadband services through an Internet access provider.*

3.3.2 Recommendations

1. Effective Statewide Planning and Coordination:

Based on a review of previous studies on funding 9-1-1, it appears that a cohesive, strong statewide 9-1-1 planning and coordinating mechanism is necessary in all states to facilitate the timely and efficient deployment of NG9-1-1 networks. Many jurisdictions have a statewide 9-1-1 coordinating body, while other states have strong and effective regional authorities in larger metropolitan areas. But some states have neither. The PSAPs fundamentally remain a local emergency communications entity within county and local governments, statewide coordinating mechanisms should play an increasingly important role in all aspects of the build-out and operations of NG9-1-1 systems. Those state level coordinating mechanisms should have responsibility for long-range planning and in-state coordination, including developing an optimal architecture for the entire state, establishing minimum service standards, and providing for training and workforce development. One clear benefit of statewide coordination is the prospect of city and regional authorities combining at least for purposes of obtaining volume and term discounts on services and equipment.

PSAPs will continue to be the operators of the 9-1-1 systems with the critical local

knowledge, and will provide the call takers and dispatchers with most of the NG9-1-1 equipment on site as well as training in its use. State law must provide a sound foundation for such a coordination mechanism, and the resulting mechanisms must be more visible and accountable. Moreover, the 9-1-1 community must develop more effective ways to engage key state decision-makers, including but not limited to the Governor, Chief Information Officers (CIO), budget offices, revenue departments, and public utility commissions, as well as key state legislators and staff responsible for emergency communications.

2. Enhanced Data Quality and Reporting:

The quality and accuracy of 9-1-1 funding data at all levels of government can be improved. Better and complete data on all aspects of 9-1-1 funding will facilitate federal and state efforts to set appropriate and sustainable levels of funding for this critical public service. Currently, the accuracy and quality of data submitted to the FCC for incorporation into the agency's annual report to Congress, required by the Net 9-1-1 Act, is deficient. State and regional 9-1-1 Authorities must work with PSAPs to improve the accuracy of the data submitted to the FCC. Moreover, the Task Force specifically recommends that (i) a third-party auditor review the data submitted to the FCC before its Net 9-1-1 Report is submitted to Congress, and (ii) third party auditing should be considered by each State as new contributor technologies/services/entities are identified, e.g., retailers for point of sale collection of 9-1-1 fees for pre-paid wireless plans and IP-enabled devices that use 9-1-1 services. As a foundational matter, audits should consider the need to develop a consensus around key terms used in the auditing process.

3. Continued Cooperative Federalism:

The concept of "cooperative federalism" must be the foundation governing the transition of existing 9-1-1 networks to NG9-1-1. Statutory authority over 9-1-1 exists at both the state and regional levels and in certain regulatory environments the FCC maintains jurisdiction. 9-1-1 calls to a PSAP that almost always originate and terminate within a state's boundaries, are *by definition* clearly both intrastate and subject to State oversight.[2] State statutes convey authority for officials to direct oversight and operation of public safety funding, deployment, and assure the responsiveness of such systems. Federal agencies, such as the FCC, DOT/NHTSA, Department of Homeland Security, Department of Justice and others, have interests in assisting in the efficient and cost-effective deployment of NG9-1-1 systems nationwide but have, in varying degrees, limited statutory authority to address certain issues or encourage certain policies. Government at all levels should engage in sustained substantive dialogue to develop additional mechanisms to promote NG9-1-1 deployment. This "big tent" approach necessarily includes disparate views and may be challenging to coordinate. But, at a minimum, the FCC should maintain its efforts to establish a long-term vision for a viable and secure NG9-1-1 network, while increasing efforts to facilitate meaningful discussions among all levels of government in order to address inconsistencies in architecture and operations among the PSAPs and states, and other jurisdictional tensions inherent in this evolving paradigm.

[2] See, e.g., the definition of "interstate services" at 47 U.S.C. §153(28) which specifically excludes from that definition: "wire or radio communication between points in the same State, Territory, or possession of the United States, or the District of Columbia, through anyplace outside thereof." Note the application of the provisions of Chapter 5 is limited by 47 U.S.C. § 152(a) to such "interstate" services and specifically excludes, as noted in 47 U.S.C. § 152(b), "charges, classifications, practices, services, facilities, or regulations for or in connection with intrastate communication service by wire or radio of any carrier."

4. State/Regional Control of PSAP Operations and NG 9-1-1 Transition:

The TFOPA endorses the need to (i) develop a state-level cost-effective, efficient architecture for NG9-1-1, and (ii) to enhance measures to protect the emergency infrastructure against cyber intrusions. The Task Force also endorses the NG9-1-1 system architecture developed to date. NG9-1-1 systems require that shared services networked across multiple PSAPs meet a series of well-defined conventional criteria.

However, such criteria should be established by a state or regional governing body and include decision analysis, cost effectiveness, budgetary constraints and priorities, accountability, and a well-defined governance structure, subject to external audits and contractual obligations. Indeed, it is crucial that PSAP and first responder operational decisions remain at the local level. This is discussed in more detail in Section 6.6 related to Effective Statewide Planning and Coordination.

5. PSAP Consolidation:

The Task Force was asked to examine prospects for greater PSAP consolidation, either within state boundaries or perhaps nationally. Consolidation is currently occurring on an organic basis. This trend towards PSAP consolidations, where it is practicable, and results in efficiency gains, is accelerating as more IP-enabled architecture is deployed and services are shared. However, as outlined in this report, there are technical, logistic, and jurisdictional challenges with any consolidation – particularly those that would occur across state boundaries. Under a cooperative federalism paradigm, state and local government authorities maintain primary jurisdiction over 9-1-1-services. Moreover, PSAP consolidation does not necessarily translate into increased efficiencies or cost savings. Therefore, the TFOPA believes that focusing only on PSAP consolidation is neither constructive nor within the exclusive scope of its work. Instead, the Task Force has chosen to focus more on which funding mechanisms offer the best approach going forward in light of the policy principles mentioned above. The recommendations in this report, as a whole, provide a more constructive path forward that is both appropriately respectful of state and local government prerogatives and legally sustainable.

6. Potential New 9-1-1 Funding Mechanisms:

The TFOPA examined five potential funding options for state and local governments with a bias towards approaches that are technologically neutral and sustainable. The results are summarized below. It is important to stress that this report presents a menu of options for the state or local government to consider when creating a longer-term approach for funding NG9-1-1 systems; it is not meant to be a federal mandate or a requirement. No funding system is perfect and adjustments will be needed for any revised funding approach, which will likely include several different funding sources. Any revision of State funding mechanisms will require some time to change current State laws and will involve a transition of several years.

A: **Approach:** *Continued reliance on the current 9-1-1 funding model supplemented by a new network connection fee on users with broadband services, and assessed on any carrier or broadband provider that provides Internet access to retail customers.*

Response: The Task Force believes this funding method is sustainable as well as technologically and competitively neutral. It could be assessed on network providers that provide Internet access in a number of different methods as described at a general level below. The details of the funding mechanism are critical, and several adjustments are needed to make this approach equitable and legally sustainable. It is recommended that further detailed study of this mechanism, and its necessary adjustments and assumptions, be carried out by a new joint

Local State Advisory Committee on 9-1-1 (as reflected by the LSAG set forth below).

B: **Approach:** *Continued reliance on the current model including efforts to secure funding from pre-paid wireless services in all states. Based on the review of the limited data available, it appears 14 states have not resolved the need to collect 9-1-1 fees on prepaid wireless plans at retail point-of-sale.*

Response: Addressing prepaid wireless plans is a crucial part of assuring sustainable and technologically/competitively neutral 9-1-1 funding. Thirty-seven (37) States have resolved the need to assess 9-1-1 on such plans after significant legislative efforts and/or litigation. However, the remaining states still need to resolve these issues. The Task Force encourages non-conforming states to resolve this "funding gap" as quickly as possible through state legislation. Also, due to the non-monthly purchase pattern of pre-paid customers, actual collections of 9-1-1 fees at point-of-sale on these plans may not be equitable at current levels. States utilizing State Comptrollers see improved performance in fee remittance and collections. As more data on actual collections is developed by state entities, and compared to forecasted collection for this class of customers, this issue will need more scrutiny. As stated above, the Task Force recommends that the FCC should refer a more detailed examination of this issue to the LSAG, or a joint advisory committee.

C: **Approach:** *Migrate 9-1-1 funding towards state universal service fee assessments. Currently, only Vermont assesses 9-1-1 fees as part of the overall funding of universal service requirements. About 22 states have some form of state-based universal service funding. At the federal level, the basis of contributions for the federal universal service program has been referred to the Federal State Joint Board on Universal Service (FCC CC Docket No. 96-45) and its anticipated report on recommended changes to the existing contribution methodology is under review.*

Response: The TFOPA concluded this is not a viable option because of the current bifurcation in how existing State universal service funds operate, and the fact that most state universal service and 9-1-1 programs are managed separately.

D: **Approach:** *Integrate NG9-1-1 funding into state sales and use taxes. About 45 states have some form of sales and use tax. However, such taxes could not be subject to the Federal proscription against diversion of 9-1-1 fees. This approach would likely reflect the problems associated with current co-mingling of 9-1-1 fees with general fund revenues, and face problems characteristic of state appropriations procedures.*

Response: The TFOPA finds less merit in this approach than did the 2015 NASNA study for several reasons. Historically, advancements in 9-1-1 were not funded by general revenue due to higher competing budget priorities, and a specialized fee concept was developed to provide dedicated funding. There is established precedent for 9-1-1 and NG9-1-1 fees to be collected separately and maintained in separate funds, outside almost all State's general fund. If combined as this approach would require, the current diversion of 9-1-1 fees will expand due to state budgetary pressures, especially among the various state agencies with some connection to "public safety" – however tenuous. Moreover, the political obstacles to enacting a sales and use tax, de novo, in the remaining 5 states would be challenging in the current fiscal environment. Some states require voter approval of new taxes, surcharges, or fee increases, while others require a super-majority (two-thirds) vote of the Legislatures to approve such fees.

E: **Approach:** *Consider incorporation of 9-1-1 funding into state insurance fees. Each state has some jurisdiction over insurance rates and policies. Some argue that*

health, fire, and casualty insurance policies also have a natural nexus to emergency communications. In fact, the Blue Ribbon Panel on 9-1-1 Funding recommended consideration of attaching a 9-1-1 fee to health insurance policies.

Response: The TFOPA did not give serious consideration to this approach because of concerns about feasibility and the gulf between jurisdictions with respect to 9-1-1, public safety, and insurance.

7. Enhance Education and Outreach:

Studies of 9-1-1 fees and NG9-1-1 deployment should be developed with a strong emphasis towards the challenges of implementation and execution. These studies should include a much more integrated, intensive approach toward outreach and education for the 9-1-1 community. These efforts should be directed toward key state decision-makers that do not generally work directly within the 9-1-1 ecosystem. Some industry stakeholders and trade associations have already developed programs to highlight the importance of 9-1-1, e.g., the National Conference of State Legislature's program and database for tracking state 9-1-1 actions. However, current efforts are not sufficient to assure timely deployment of NG9-1-1, yet more can be done. The FCC's Bureau for PS/HS, NASNA, NARUC, NENA, APCO, DOT/NHTSA, along with state and local public safety stakeholders need to develop a coordinated plan to educate key decision-makers.

8. Creation of a Local State Government Advisory Committee on 9-1-1 (LSAG):

Federal/State advisory committees have been established to address a variety of issues. One possibility is to convene a Local State Government Advisory committee to focus solely Next Generation 9-1-1 issues. The goals of such a committee would include the development of messaging points and information for local, state and federal entities to understand NG9-1-1, funding and policy recommendations and more. Moreover, within the authority of the Commission, the committee could examine in more depth, with an eye toward effective implementation, some of the recommendations in this report, including the network connection fee, the alleged under-recovery of forecasted revenues from pre-paid wireless plans, how to enhance the quality and analysis of the data submitted to the FCC and subsequently to Congress pursuant to the Net9-1-1 Act, and other issues.

4 Optimal Approach to Cybersecurity for PSAPs

4.1 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 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. The Task Force 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. The TFOPA was also challenged to examine this same cybersecurity issue for tomorrow's PSAPs, in the context of NG9-1-1 systems and services.

This part of the 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 NG9-1-1 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, the TFOPA 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. The TFOPA 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, the TFOPA 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 later in this 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 the TFOPA 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 this section of the report, the TFOPA has created three (3) appendices that support it. The first is a set of use cases that are pertinent to PSAPs not only in an NG environment, but also 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 the TFOPA that the following work product will be of use to PSAPs around the Nation and to all emergency communications partners.

4.2 Objective, Scope, and Methodology

4.2.1 Objective

The objective of the Task Force was 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 Communications Security, Reliability and Interoperability Council (CSRIC) IV and DHS; industry specific standards bodies such as NENA, APCO, and ATIS; and commercial industry best practices.

Part of the objectives for the Task Force was 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 also 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.

4.2.2 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), the TFOPA incorporated the work of these outside agencies and organizations into the proposed recommendations to the Commission. In addition, the Task Force made an effort 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, but also the human factor is critical. 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.

4.2.3 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 reflected in Section 5 also will be referenced here as the TFOPA 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 TFOPA 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 Task Force will also leverage the NICE Workforce Framework to provide guidance for PSAP cybersecurity workforce development and training plans.

4.2.3.1 Use Case Methodology

The TFOPA 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 Task Force 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 to public safety in general, that cybersecurity is a very real concern. By demonstrating high level vulnerabilities and risks, it is the hope of the Task Force 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.

4.3 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 Section 5 of this 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 Section 5 of this report will delve into architectural options, this section of the report will not consider each option individually. Instead, this section will address cybersecurity from an enterprise point of view. PSAPs, 9-1-1 Authorities and local agencies will then have information from both sections of this report to help address ways to defend their architecture choice regardless of what that specific choice is.

The TFOPA 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.

4.3.1 Current PSAP environment – Cybersecurity Today

In this section, the TFOPA 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 IV Working Group 2A provide insight into relevant security issues and are critical to current as well as future operations.[3] These documents are discussed in detail later in this report.

4.3.1.1 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

[3] [Cybersecurity Best Practices, March 2011]

security risk.[4]

4.3.1.2 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).

4.3.1.3 Compliance

A clear understanding of all applicable information security requirements is imperative to ensuring compliance. Regular internal and/or external audits are conducted to measure compliance with all laws, regulations, customer requirements, and subscribed best practices.

4.3.1.4 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.

4.3.2 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."[5]

4.3.2.1 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.

4.3.2.2 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

[4] See "Security management system's usability key to easy adoption". sourcesecurity.com.
[5] See: http://c.ymcdn.com/sites/www.nena.org/resource/resmgr/Standards/NENA_04-503.1_Network_System.pdf

systems should be controlled via the appropriate passwords and certificates.

4.3.2.3 Human Resources

Human Resource (HR) procedures should be developed to include preventative measures such as background checks. Procedures should acknowledge that job rotations might 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.

4.3.3 Security Controls

What follows are specific methods for protecting information assets.

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

The protection of information assets must include a detailed plan for business disruptions and instructions for recovery and resumption. This includes the identification of information security concerns in emergency situations.

4.3.3.2 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.

4.3.3.3 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.

4.3.3.4 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.

4.3.3.5 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.

4.3.3.6 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.

4.3.4 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.

4.3.4.1 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 Domain Name System (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.

4.3.4.2 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 specification identifies specific firewall and Session Border Control functions necessary to facilitate secure access.

4.3.4.3 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 Signal Transfer Point (STP). The purpose is to ensure that only messages specifically required for emergency services implementations are allowed to pass.
2. IP data entry points (Session Initiation Protocol (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 Internet Protocol Security (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.

4.3.5 Transitional NG9-1-1 Architectures

As previously noted, this section of the report will not delve into specific architecture discussions. However, in order to mirror the approach reflected in Section 5, it is noted 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 Selective Router (SR) with an IP infrastructure and continues to process 9-1-1 calls based on the callers Automatic Number Identification (ANI) and a mapped Emergency Services Number (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 Section 5 of this 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.

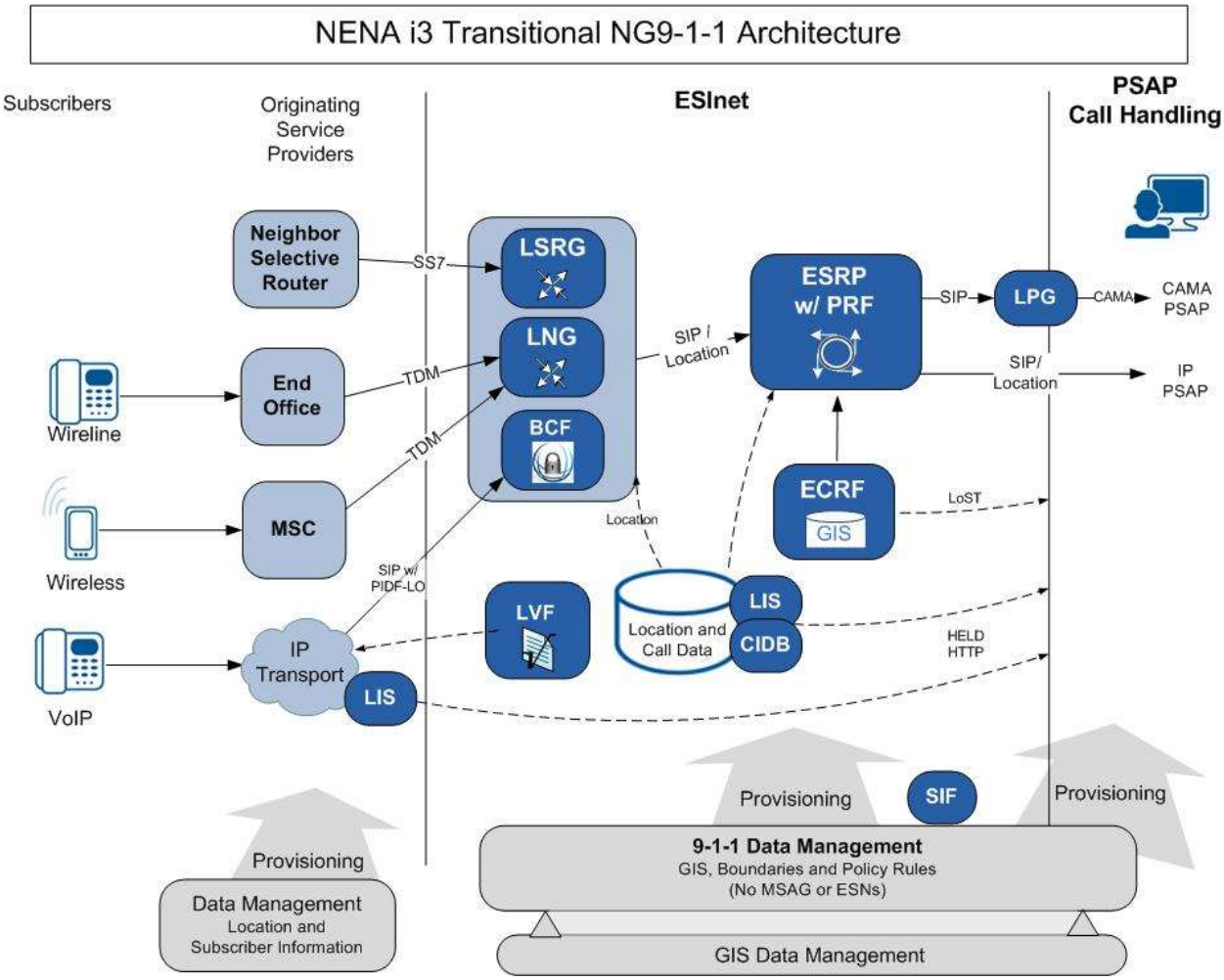


Figure 4-1 - NENA i3 Transitional NG9-1-1 Architecture

4.3.6 IMS and ESInets

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).[6]

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 Section 5 of this 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, the TFOPA 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 The 3rd Generation Partnership Project (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

[6] 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 Uniform Resource Identifier (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 where the call will be delivered. The LRF may use internal processes to access an integrated Routing Determination Function (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." [7]

Figure 4-2, 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.

[7] ATIS-0700015.v003, Applying common IMS core elements to ESINet architecture

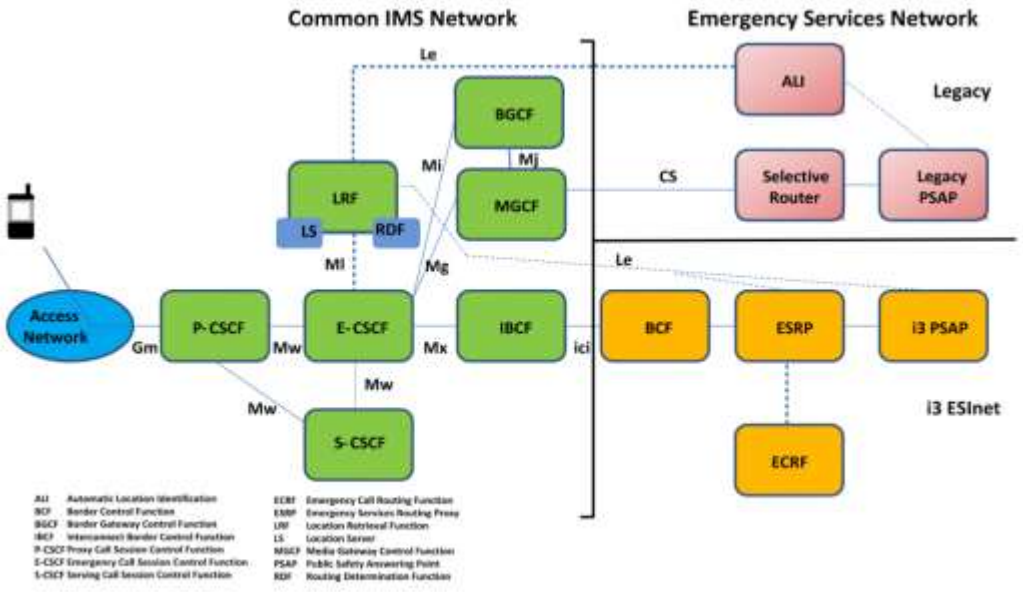


Figure 4-2 - IMS to ESINet diagram

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 the TFOPA 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.

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

4.4.1 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.

The TFOPA 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 Figure 4-3 below, the Task Force 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 anomolies and events that exceed predetermined thresholds. Those identified channels will detemrine 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 4-3 - NIST Framework Core with Implementation Levels

4.4.2 Security Considerations for Applications (Apps) Interfacing To/With Public Safety

The 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.[8] The NIST summary is offered only as reference and does not represent any endorsement by the TFOPA 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.

4.4.3 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 documents and the 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.[9] 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.

4.4.4 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.

4.4.5 ICAM Intersection

Understanding that the 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

---

[8] Public Safety Mobile Application Security Requirements, Workshop (2/25/2014), available at http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8018.pdf.

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

solutions that enable strong and dynamic processes. In fact, one of the primary dependencies across both the 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 credentialed, 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 the ICAM, the following challenges have emerged to the adoption of a consistent approach to the 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 Return on Investment (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 the 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 the ICAM will help to resolve the significant IT, security, and privacy challenges facing multiple levels of government.

When properly aligned, the 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, the 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 the 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.

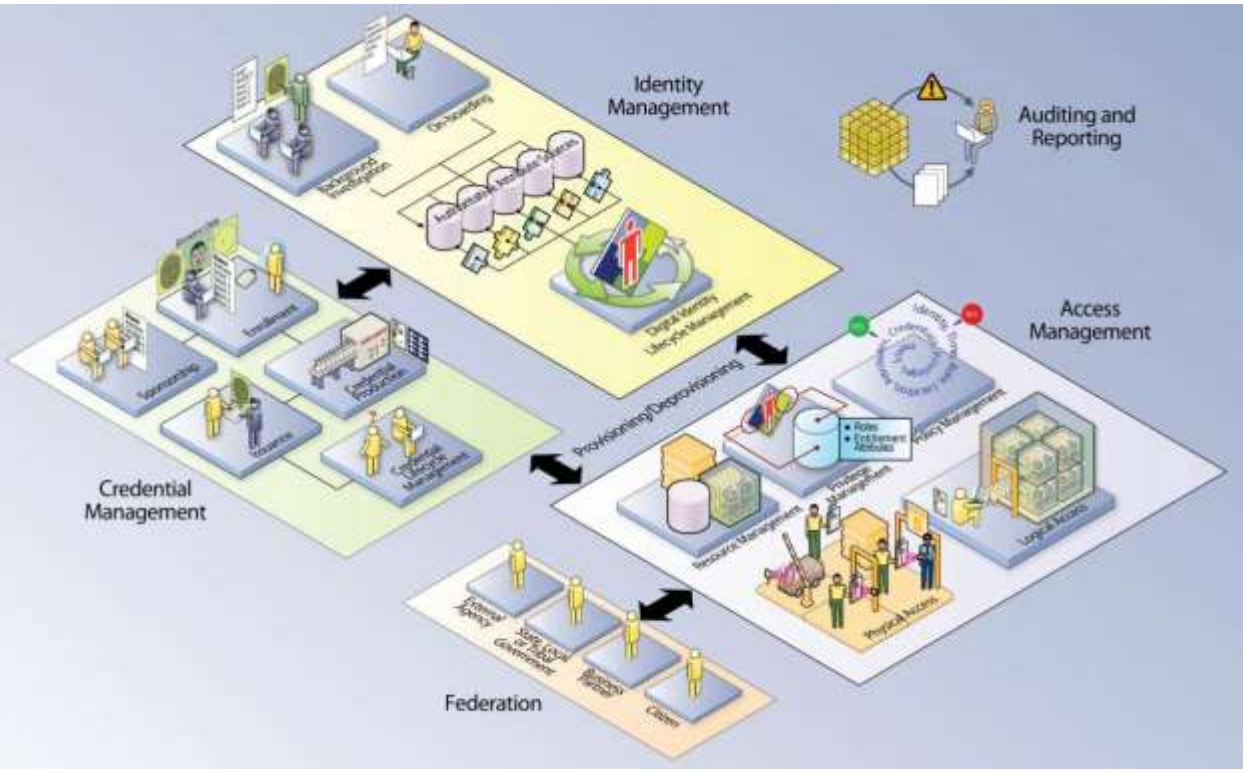


Figure 4-4 - ICAM "Big Picture"

4.4.6 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 4-5 - Federal ICAM Roadmap

4.4.7 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 4-6 - Levels of Identity Assurance

4.4.8 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) communications 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.

4.4.9 Credential Management

According to the 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.

4.4.10 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 is often viewed as the most significant parts of the ICAM from a 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.

4.5 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.[10]

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

[10] A comprehensive application of the Workforce Framework is beyond the scope of TFOPA. 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

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:

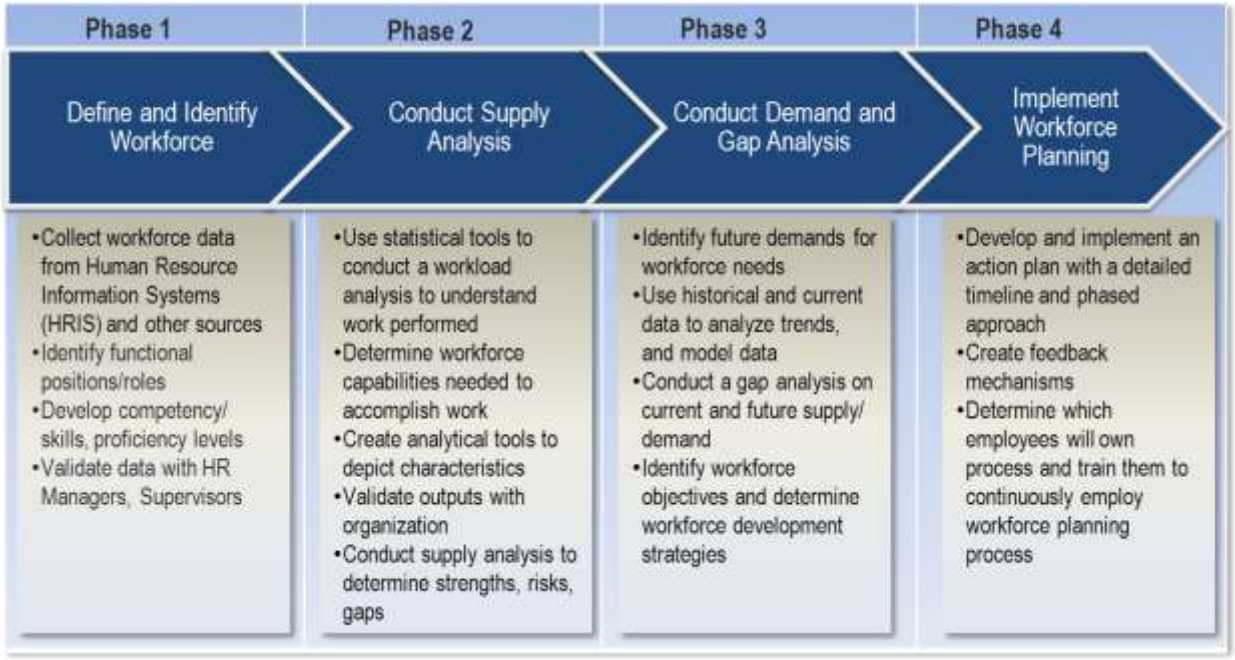


Figure 4-7 – Workforce Planning Process

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, Task Force members reviewed job titles, roles and skills to assess the 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:

PSAP job titles:	Category	Scope of Work	Required Skills (IT Related)	Example Training
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 Cybersecurity 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 Cybersecurity 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 Cybersecurity 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 Cybersecurity for Managers - Security +

PSAP job titles:	Category	Scope of Work	Required Skills (IT Related)	Example Training
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 the computerized 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 Cybersecurity 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 the computerized 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 Cybersecurity 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 Cybersecurity for Managers

PSAP job titles:	Category	Scope of Work	Required Skills (IT Related)	Example Training
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 Cybersecurity for Managers - Network + - Security + - IR Framework - CISSP

PSAP job titles:	Category	Scope of Work	Required Skills (IT Related)	Example Training
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

4.5.1 DHS Recommendations and Resources

The TFOPA representatives from the U.S. Department of Homeland Security (DHS) contributed the following section. The 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.

The 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.

4.5.1.1 Technical Programs

The 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 NCCIC is a 24/7 cyber monitoring, incident response, and management center.[11] 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.[12]

Federal, State and Local Partnerships and Forums. The DHS has formed existing relationships across all levels of government to inform the design and deployment of Emergency Communication1 networks. The DHS supports SAFECOM and the National Council of Statewide Interoperable Coordinators bringing State, local, Tribal, and Territorial perspective to a National forum. DHS has partnered with the U.S. Department of Transportation (DOT) NG9-1-1 Program Office to facilitate education and awareness of cybersecurity with the State and local community through the delivery of tools and training. The 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.[13] Additionally, DHS manages the Emergency Services Sector (ESS) Cyber Working Group to evaluate cyber risks that the sector might encounter.[14]

Assessments and Analysis. The 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.[15] Additionally, the DHS is

[11] 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
[12] National Cyber Awareness System, https://www.us-cert.gov/ncas.
[13] Office of Emergency Communications, http://www.dhs.gov/office-emergency-communications.

[15] Cyber Risks to Next Generation 9-1-1, available at http://www.dhs.gov/office-emergency-

working on next steps on the development of Identity, Credential, and Access Management (ICAM) for public safety and FirstNet's National Public Safety Broadband Network. The through the ESS Cyber Working Group mentioned above, the Department has published the DHS Internet Protocol (IP) Emergency Services Sector Cyber Risk Assessment and Emergency Services Sector Roadmap to Secure Voice and Data Systems 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.[16] [17]

Public / Private Collaboration. The Critical Infrastructure Cyber Information Sharing and Collaboration Program (CISCP) establishes trusted cyber information sharing relationships across Government and Industry. The CISCP facilitates the secure exchange of cybersecurity indicators, enabling organizations to protect themselves against emerging attacks. Currently, the CISCP has over one-hundred member organizations and is working in collaboration with the NCCIC to automate cybersecurity information sharing amongst its members.[18]

User Training and Education. The 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.[19] The DHS also supports the National Initiative for Cybersecurity Education (NICE), which provides additional educational resources for public and private organizations.[20] The 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 (C^{3}VP) supports organizations of all sizes to establish or improve their cyber risk management processes and to take advantage of free technical assistance, tools, and other resources offered by the U.S. Government. C^{3}VP can assist PSAPs in understanding how to use NIST's Cybersecurity Framework and other risk management efforts.

4.5.1.2 Technical Solutions

The 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

---

communications.

[16] 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

[17] ESS Roadmap to Secure Voice and Data Systems. https://www.dhs.gov/sites/default/files/publications/Emergency-Services-Sector-Roadmap-to-Secure-Voice-and-Data%20Systems-508.pdf

[18] (https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity)

[19] (http://www.dhs.gov/stopthinkconnect)

[20] (http://csrc.nist.gov/nice/index.htm)

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 (TIC)	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 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 System (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 System (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, and 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.

4.5.2 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 IV created ten working groups, each with its own area of responsibility.

The 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.[21] WG4

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

also was charged with providing implementation guidance to help communication providers use and adapt the NCF. The TFOPA supports the use of NIST CFS as recommendation as they apply in the final CSRIC IV 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.

4.6 Proposed Approaches to NG9-1-1Cybersecurity Architecture

4.6.1 The Emergency Communications Cybersecurity Center (EC3)

In addition to incorporating current best practices, the NIST recommendations, and current work from DHS, APCO, ATIS and NENA, the TFOPA 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.

4.6.2 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 Intrusion Detection System (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.**
  - The 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 the 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 of the IDPSs do not. Most of the 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.

4.6.3 Proposed *A*pproach for IDPS in the NG9-1-1 *E*nvironment

In the proposed NG9-1-1 architecture, the Emergency Communications Cybersecurity Center (EC3) will take on the role of providing the 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 also 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 which support the Core Services elements and operates 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 also is 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 these data flow, and cooperative approach, might present are included in Figures 4-8 and 4-9 on the following pages.

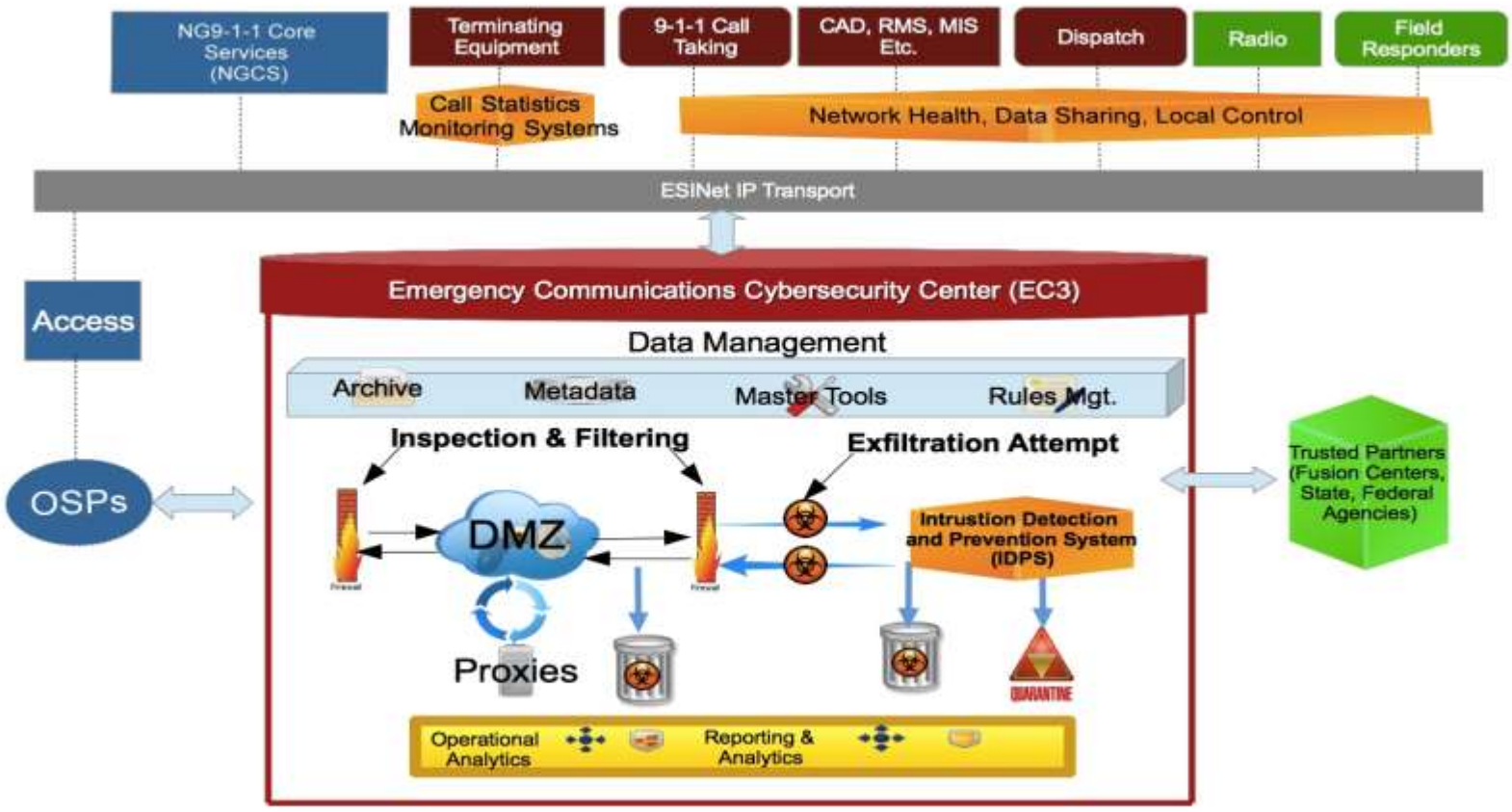


Figure 4-8 – Proposed Architecture for Emergency Communications Cybersecurity Center (EC3)

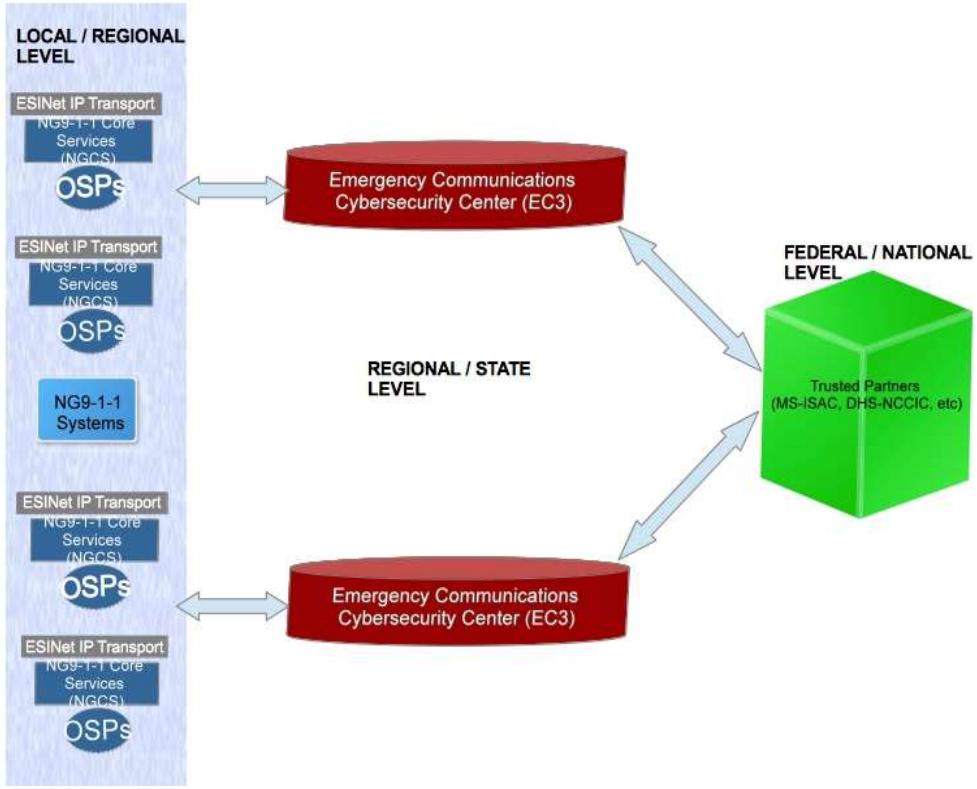


Figure 4-9 - EC3 Information Flow Example

4.6.3.1 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 the TFOPA is not endorsing any specific vendor, product, or organization the model provided by the 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, the TFOPA received input and assistance from representatives of the MS-ISAC.[22]

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 federal government's ability to understand mission impacts on emergency communications. It is

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

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 (LEC), or named wireless service providers, as observed in Virginia during the Derecho, or after an Earthquake. The 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 the CalOES is capable of providing constant and continual monitoring of the ECATS dashboard, deployed by the CalOES across the entire State of California. In this capacity the NCC and NCCIC can coordinate with the 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.

In the case of the MS-ISAC, sensor data is routed to the MS-ISAC, triaged and reported to the NCCIC as needed. 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 State, Local, Tribal, and Territorial (SLTT) entities being monitored.

This approach allows the NCCIC to provide EC3's and PSAPs 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 to best design, build, and defend these emergency communications cybersecurity systems as a cooperative effort between public safety and industry.

4.6.3.2 Cost Considerations

4.6.3.2.1 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 Task Force 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 TFOPA 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 TFOPA 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

4.6.3.2.2 Capital Costs and Considerations

The building out of the EC3 should be a very similar per-square-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 Task Force 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 re-purposing 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 build-out, 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 TFOPA does not have price estimates for such a deployment, they could be obtained by contacting the CalOES officials directly.

4.6.3.2.3 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 6000 PSAPs in the United States be burdened with building and staffing such facilities, the TFOPA 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.

The TFOPA 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 the limited timeline in which to complete the TFOPA report, the Task Force 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, the TFOPA recommends additional study on costs, available solutions, and potential partnerships.

4.7 Recommendations

The Task Force'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.

- The TFOPA 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. The CISCP facilitates the secure exchange of cybersecurity indicators, enabling organizations to protect themselves against emerging attacks. Currently, the 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 from which to build. 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 TFOPA 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 the limited timeline in which to complete the TFOPA report, the Task Force 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, the TFOPA recommends additional study on costs, available solutions, and potential partnerships.

- Governance is pivotal to secure and interoperable emergency communications. The TFOPA 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. The TFOPA recommends that as part of any follow on work future iterations of the TFOPA consider how governance applies to, or impacts, the effective creation of collaborative cybersecurity solutions.
- The TFOPA 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 4.4.1, Figure 4-3 of this report, the Task Force has detailed both the recommended implementation level and high-level requirements to attain the stated goal. It is recommended 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 the 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 Task Force recommends that PSAPs and 9-1-1 Authorities use the included chart as a baseline document for identifying training needs and planning accordingly. In addition, as the Task Force was somewhat limited on time to further study this area, additional work may be merited by future iterations of the TFOPA.
- The ICAM is critical to the success of any cybersecurity solution and system. The TFOPA recommends that from the PSAP level, up through any proposed cybersecurity core architecture, and on into the Federal space the 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.

  The TFOPA has limited its 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. The TFOPA supports PSAP and 9-1-1 Authority implementation of multi-factor authentication at the PSAP level and inclusion of the 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 Section 5.

- As discussed in Section 5, there are a number of governance and architecture issues along with expected "roles" within the NG9-1-1 ecosystem. The TFOPA recommends that PSAPs and 9-1-1 Authorities conduct a logical analysis of each potential architecture option as recommended by Section 5, and then consider integration of the core cyber services, local PSAP workforce, and the ICAM recommendations, and collaborative information and data sharing as part of the overall NG9-1-1 implementation process.
- The TFOPA 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.
- The TFOPA 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. The TFOPA 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, the TFOPA 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.

4.8 Cybersecurity Summary

The TFOPA 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 the efforts to defend next generation networks and systems. The actors, vectors, and outcomes for cyber-attacks against public safety vary widely, and therefore, our approach to defending against these attacks must be focused.

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 the TFOPA believes the entire public safety enterprise should consider. Data from deployed sensors could route back to entities such as the NCCIC and MS-ISAC, or 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.

The TFOPA 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 believed 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 the TFOPA, or the TFOPA related activities. In conducting this work, the TFOPA 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, the TFOPA 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. The TFOPA believes the information and recommendations contained in this report provide foundational work upon which such systems can be based, and built.

5 *Optimal Approach to NG9-1-1 Architecture Implementation by PSAPs*

5.1 Introduction

5.1.1 The Emergence of 9-1-1 for a Nation: History of 9-1-1

Emerging NG9-1-1 environment since the late 1960's, the 9-1-1 system has been advancing and evolving throughout the United States. Throughout the years, 9-1-1 has stood as the sole number for notifying a Public Safety Answering Point (PSAP) that an emergency is occurring and the caller needs law enforcement, fire, or emergency medical assistance from emergency responders. Based on the telephone network that existed, it was logical to use a feature known as "selective call routing" to support the implementation of 9-1-1 calling through central offices, nationwide. Backed by Congress and various other industry groups, E9-1-1 systems and networks supporting 9-1-1 calling spread across the nation.[23]

Information provided by NENA, The 9-1-1 Association states:

- By the end of 1976, 9-1-1 was serving about 17% of the population of the United States. In 1979, approximately 26% of the population of the United States had 9-1-1 service, and nine states had enacted 9-1-1 legislation. At this time, 9-1-1 service was growing at the rate of 70 new systems per year. By 1987, those figures had grown to indicate that 50% of the US population had access to 9-1-1 emergency service numbers.
- At the end of the 20th century, nearly 93% of the population of the United States was covered by some type of 9-1-1 service. Ninety-five percent of that coverage was E9-1-1. Approximately 96% of the geographic US is covered by some type of basic 9-1-1 or E9-1-1. The rest use remote call forwarding of 9-1-1 to a ten-digit number at a selected answering point.

In the 1980s, the telephone companies' "Operator Services" technology was adapted for 9-1-1 providing the PSAPs with the caller's telephone number, commonly known as Automatic Number Identification (ANI). Dedicated 9-1-1 networks utilizing circuit switched Selective Routing (SR) functionality accommodated the need for routing of 9-1-1 calls to differing jurisdictions. Telephone company customer records contained specific address information that correlated to the telephone number enabling 9-1-1 Authorities to partner in 9-1-1 database development of what is known today as Automatic Location Identification (ALI). The technology adaptations became the norm for 9-1-1 services deployed throughout the United States establishing the Enhanced 9-1-1 features commonly referred to as ANI/ALI/SR. Although cell phone technology existed as early as 1973, it was not until the mid-nineteen eighties that the next major step occurred in mobile phone technology with the First Generation (1G) fully automatic cellular networks introduction. In 1983 the FCC licensed cellular service provider began the first ever mobile phone service and the evolution of cellular technology began eventually leading to wireless 9-1-1 service. It was at this point that, the telephone number to

[23] Status of Legislation Concerning 9-1-1 The Emergency Telephone Number, U.S. Dept. of Transportation; U.S. Dept. of Commerce, NTIA. July, 1979. Archived – National Emergency Number Association.

dispatchable address correlation became invalid, as numbers became mobile with the device and no longer fixed to a specific address. Mechanisms were developed to accommodate cellular 9-1-1 in the wired landline E9-1-1 model, and while it provided a stopgap measure, each technology advancement in cellular deployment widened the gap between the technology and the solution. Compounding the complexity of the problem further, the advancement and acceptance of Voice over Internet Protocol (VoIP) technology introduced a new era. Communication challenges for 9-1-1 continued to emerge, as fixed devices became nomadic and mobile cell phones entered into the IP digital age where both data as well as voice was seamlessly delivered.

In 2014, CTIA reported that US cellphone penetration surpassed the population by 10%, indicating that there were more wireless connections than recorded population.[24] With nearly everyone, teenager to older adult, possessing some form of cellular technology, they hold the key to immediate 9-1-1 access in the palm of their hand. 9-1-1 calling behaviors began to change and the exponential growth in cellular and IP technology continues to strain the 9-1-1 network. The FCC estimates that over 70% of all 9-1-1 calls are placed from wireless phones. Selective routing provided through analog technology is rapidly moving toward extinction. IP based technology is essential for the future.

Throughout the U.S. the legacy forty-year-old 9-1-1 solutions cannot support the needs of advanced communication technologies. Public expectations are changing and new technology will afford public safety the opportunity to provide more effective emergency response. We must embrace a new approach to keep pace with evolving consumer communication services and emergency response needs.

5.1.2 Emerging NG9-1-1 Environment

This report is designed to provide an overview to emerging NG9-1-1 systems, sets the stage for better insight into the system descriptions, and allows for an analysis of PSAP and NG9-1-1 architecture optimization. This report is structured to provide a thorough understanding of Public Safety Answering Point (PSAP) and NG9-1-1 operational models and includes an objective analysis of operational efficiencies gained through upgrading to more advanced technologies. In contrast, the authors of this report also included administrative challenges that could exist when planning for NG9-1-1.

Throughout this report the reader will find that NG9-1-1 introduces a more efficient, precise technical infrastructure for handling 9-1-1 emergency requests through intelligence inherent in the technology. For example, the system when fully implemented, will completely change the way 9-1-1 calls, or requests for assistance are routed. Greater intelligence in the call routing functionality will minimize the need to transfer a call to the correct PSAP, which is a normal operational occurrence today in legacy 9-1-1 systems. Location-based call routing allows the location data of the individual initiating the 9-1-1 request to more precisely route to the PSAP responsible for the service request.

The NG9-1-1systems enables the general public to have options beyond voice and Teletypewriter/Telecommunications Device for the Deaf (TTY/TDD) regarding how they contact 9-1-1 Centers for emergency assistance, and can also allow for providing additional data

[24] "Annual Wireless Industry Survey" http://www.ctia.org/your-wireless-life/how-wireless-works/annual-wireless-industry-survey. CTIA, June 2015. Web. Last Accessed 12/03/2015.

beyond what is transmitted to 9-1-1 today. Texting, sharing photos and establishing video calls are now commonplace in this society and it is logical to create a 9-1-1 system that accommodates these applications. In addition, it is critical that individuals with speech or hearing disabilities have a method, other than TTY/TDD, to contact 9-1-1. Next Generation 9-1-1 will establish the underlying technical platform and functional applications to phase in these technologies.

As stated earlier, the legacy 9-1-1 systems deployed throughout the United States today are limited and cannot fully support the advanced communication technologies used by the general public. Upgrading legacy 9-1-1 systems require knowledge of the technological advancements in 9-1-1, evaluation of 9-1-1 service optimization options, and development of a well-coordinated plan. The following sections of this report are designed to provide the foundation for planning, integration and implementation of NG9-1-1.

5.2 Objective, Scope, and Methodology

The Intent of This Work: With the evolution of 9-1-1 technologies, it is clear that the term "Next Generation 9-1-1" needs to be better understood by all stakeholders. Many organizations and industry authorities have contributed to the development of NG9-1-1, and several well respected reports were completed in the early stages of the evolution. What was lacking in these efforts however was an overall comprehensive understanding and roadmap pooling of the disparate "facts" into a single resource that would provide guidance to decision-makers as they moved forward with their vision and ideas.

This introduces several questions concerning the optimal architecture for NG9-1-1:

- Is there one "best and optimal design"?
- If so, what are the elements required for that design?
- If not, what are the various configurations that could be combined together to reach that optimal objective?
- And how do you best accomplish the transition from legacy to NG9-1-1?

These and many other questions have been confronting decision-makers as they consider the transition to NG9-1-1. The attempt to correlate and understand competing information is creating confusion.

To clarify this confusion, this report addresses various optimal architectures for NG9-1-1. By reading this report, decision-makers tasked with the challenges of making choices for design and configuration of their 9-1-1 systems and will be capable of understanding not only the key decision factors, but also the broader understanding of the relevant impact of those decisions.

The TFOPA does not believe there is a single best system design, but rather various options that may be selected representing an "optimal architecture" for each specific NG9-1-1 system. The intent of this report is to create a road map that identifies the components and optimal configuration choices available to decision-makers. These configuration choices include access for the originating service providers, NG9-1-1 core services, ESInet, and the call-taking and dispatching infrastructure. Emergency response and incident management are outside the scope of this report.

This report provides criteria and comparative information to 9-1-1 Authorities and related stakeholders at all levels of government, so they can determine what choices best meets their respective needs.

5.3 Current PSAP Decentralized Environment

The decentralized PSAP environment is prone to fragmentation and duplication. Optimization opportunities for this environment, while still maintaining its decentralized characteristics, are limited and challenging. However, options such as utilizing virtual PSAP arrangements, network-based terminating equipment, and network-based support systems (CAD, MIS, Recording, etc.) can be applied without changing the local structure of PSAPs. Essentially the sharing of such infrastructure can result in a single virtual PSAP scenario or continued independent operation through use of multi-tenancy.

5.3.1 Decentralized Environment Characteristics

5.3.1.1 PSAP Infrastructure Elements

In the typical legacy environment, PSAP equipment and software are predominantly located within the boundary of each PSAP (though remote positions associated with a particular PSAP may be present). The list of functional elements (FE) is comprised of but not limited to the list below. A simplified diagram illustrates the connections:

Typical Legacy 9-1-1 Functional Elements

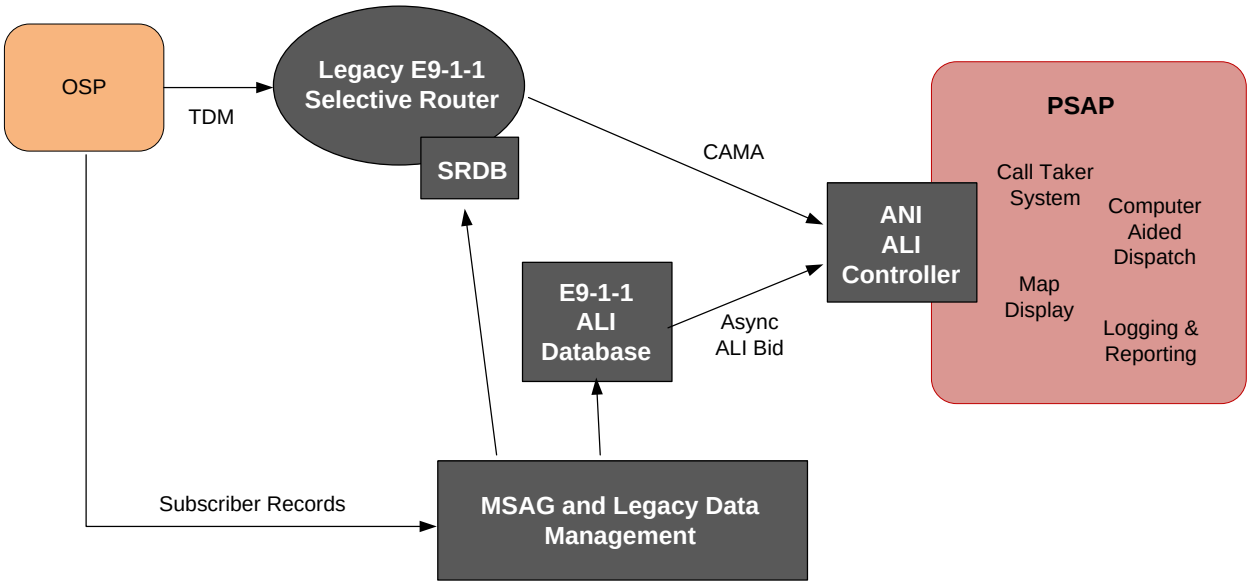


Figure 5-1

Administrative Phone System: The Administrative phone system includes telecommunication equipment that handles processing of administrative telephone communications.

Automatic Location Identification (ALI): The automatic display at the PSAP of the caller's telephone number, the address/location of the telephone and supplementary emergency services information of the location from which a call originates. The ALI Database is a set of ALI records residing on computer servers.[25]

[25] NENA Master Glossary of 9-1-1 Terminology, 2014

PSAP Phone System/Customer Premise Equipment (CPE) : Equipment used for handling emergency 9-1-1 and non-emergency calls for service. Manages all communication from the caller, and includes the interfaces, devices and applications utilized by the 9-1-1 Telecommunicator to handle the call. This can also include administrative telephone systems used within an agency but not integrated into the 9-1-1 equipment.

Computer Aided Dispatch (CAD): An integrated technology solution for management of public safety incident creation functions associated with emergency and non-emergency calls for assistance, dispatch of first responders and incident tracking. The CAD also operates as a connection to other information sources and databases through various interfaces built into the system such as, but not limited to:

- National, State, Regional or local databases
- Emergency Medical Dispatch software or card system.

Geographic Information System (GIS): A system that allows for mapping, model, query and analysis of spatial or geographical data.

Instant Recall Recorder (IRR): A device that enables the playback of recent audio conversations and radio traffic related to emergency communications.

Local Area Network (LAN): The local area network within the PSAP. There can be multiple networks, with multiple sub-nets and IP schemas.

Logging Recorder: The technology used for **r**epository of emergency incident communications and related voice data.

Management Information System (MIS): The MIS system provides reporting services based on data collected from other FEs.

Map Database: Stores a set of data layers obtained from a GIS and provides a query function that returns a set of features within a defined boundary that may be used to create a map for display.

Records Management System (RMS): An agency-wide system that provides for the storage, retrieval and retention, archiving and viewing of, information, records, documents or files pertaining to public safety operations. The RMS covers the entire lifespan of public safety records development from the initial generation to its completion.

System Alarms: A mechanism to provide notification to internal or external entities of system errors, failures, or other conditions of interest.

Time Server: A Functional Element that provides Network Time Protocol (NTP) time services to other Functional Elements.

Wide Area Network (WAN): The wide area network the PSAP must access for connectivity to external resources including but not limited to hardware and data services.

5.3.1.2 PSAP Structure & Governance

In March 1973, the White House's Office of Telecommunications issued a national policy statement that recognized the benefits of 9-1-1, encouraged the nationwide adoption of 9-1-1, and provided for the establishment of a Federal Information Center to assist units of government in planning and implementation.[26] Units of government, usually cities and counties, across the United States began implementing 9-1-1 for their citizens, which led to the creation of a large number of Public Safety Answering Points (PSAPs) across the United States. This initial approach enabled a wide variation of governance models.

Over time, and for various reasons, the number of PSAPs has declined in some locations. For example, in 1981 Oregon had over 280 PSAPs and today there are 43.

The decline in the number of PSAPs across the nation can be attributed to the formation of other governmental mechanisms serving several jurisdictions at a:

- county
- regional, or
- state level

Some PSAPs have also joined together to share equipment, services, and resources through:

- Shared infrastructure such as CPE, Controllers, CAD systems, recording systems, notification systems, etc.
- Shared resources for training, GIS and Master Street Address Guide (MSAG) maintenance, 9-1-1 call taking and processing, etc.

However, there are still many PSAPs serving a single jurisdiction and are managed by the city, county, police, or fire department they serve. In some areas these single jurisdiction PSAPs have joined together under a joint management structure while maintaining their independence serving their jurisdiction.

Governance of any of these structures must be based on what works best for those involved. The governance and management of joining together as described above must be based on an intergovernmental agreement of the parties involved. The form of the agreement should be based on state statutes or local ordinances. The agreement should identify the management of the agreed upon services, and establish performance standards for what is considered successful program performance.

5.3.1.3 PSAP Operations

The PSAPs operate independently and autonomously. Operations of a PSAP are typically handled within the confines of the PSAP itself and are dependent on serving those agencies identified within the PSAPs 9-1-1 Service Plan.

The PSAPs perform varying functions based on the local agencies it serves. The PSAPs must tailor Standard Operating Procedures (SOPs) around the utilization and support of the PSAPs basic functions and the infrastructure elements outlined in 3.1.1.1. The PSAPs are responsible to answer, arbitrate and coordinate appropriate responses to emergency requests received by the PSAP. The services provided by a PSAP will vary based on PSAP type (primary or secondary), managerial functions, fiscal appropriations, interoperability, and local control. A

[26] National Emergency Number Association, archives.

PSAP receives emergency requests for service in a variety of mechanisms and channels. There is an initial alert that occurs, followed by information delivery. The media of the information could be delivered via audio, data or text and the PSAP uses several systems to process emergency calls as defined in Figure 3-2 below:

METHODS FOR ACCESSING PSAP	9-1-1 TECHNOLOGY USED BY PSAPs	PSAP DISPATCH RESOURCES	COMMENTS
Wireline (Home, Business, etc.)	Basic 9-1-1, Enhanced 9-1-1, NextGen9-1-1*, 10-digit Emergency Lines, TTY/TDD	Emergency Dispatch Protocols, Computer Aided Dispatch, Enhanced External Data Sources, GIS Systems, Emergency Notification System	Additional Data Sources (i.e., Smart9-1-1) Reverse Notification Systems (i.e., Code Red, Reverse 9-1-1, Everbridge, etc.)
Wireless (Mobile Devices)	Basic 9-1-1, Enhanced 9-1-1, NextGen9-1-1, 10-digit Emergency Lines, TTY/TDD	Emergency Dispatch Protocols, Computer Aided Dispatch, Enhanced External Data Sources, GIS Systems, Mobile Device Applications, Emergency Notification Systems	
Text	Web Client, TTY/TDD, or Integrated into 9-1-1 Equipment	Emergency Dispatch Protocols, Computer Aided Dispatch, Enhanced External Data Sources, GIS Systems, Mobile Device Applications	
Telematics	Basic 9-1-1, Enhanced 9-1-1, NextGen9-1-1	Emergency Dispatch Protocols, Computer Aided Dispatch, Enhanced External Data Sources, GIS Systems	
Relay Centers	Basic 9-1-1, Enhanced 9-1-1, NextGen9-1-1, 10-digit Emergency Lines, TTY/TDD	Emergency Dispatch Protocols, Computer Aided Dispatch, Enhanced External Data Sources, GIS Systems,	
Social Media	Basic 9-1-1, Enhanced 9-1-1, NextGen9-1-1, 10-digit Emergency Lines, TTY/TDD	Emergency Dispatch Protocols, Computer Aided Dispatch, Enhanced External Data Sources, GIS Systems,	

Figure 5-2

The PSAP Operations encompasses a multitude of technologies and information sources as identified above, and these sources are used to process a variety of emergency calls on a daily basis. The various calls can range from someone calling for assistance from their home or office; to an alarm company advising on a critical alarm status; to an automobile involved in a collision needing emergency assistance. The combination of technologies, information sources and skilled 9-1-1 personnel are what make a difference in dispatching emergency response to save a life or protect property.

5.3.1.4 Legacy PSAP to PSAP Communication

The current definition of "Interoperability" by the U.S. Department of Homeland Security is "To enable the emergency response community to communicate and share information across levels of government, jurisdictions, disciplines, and organizations for all threats and hazards, as needed and when authorized."

Most legacy PSAPs are stand-alone entities and very autonomous. As a result, local telecommunications interoperability among PSAPs operating in this environment is limited to the transfer of calls to another PSAP that has been pre-identified by the PSAPs involved, and arranged through the serving Local Exchange Carrier (LEC). In some legacy PSAP environments the public telephone switch telephone network is used for call transfer of emergency calls and does not include the transfer of critical data such as caller telephone number or address location. Such limitations can impact the dispatch of emergency services. Legacy 9-1-1 technology also struggles with receiving text, expanded data and wireless location information that is commonly available today. A "Band-Aid" solution to the old legacy technology is no longer sufficient and the limitations continue to impact sharing of information impeding incident situational awareness among multiple responding services. For example, multiple physical radios placed in a police unit or fire apparatus to serve mutual aid agreements with adjacent jurisdictions. While some of these obstacles have been overcome in some regions, it continues to be a problem for the majority.

5.3.1.5 PSAP Optimization Considerations and Factors for the Decentralized Environment

Optimization: Making the best, of anything. Many think PSAP optimization means consolidation. However, in a decentralized environment PSAPs can make the best of that environment in several ways.[27] They can judge that decision based on:

- Does it make sense
  - Operationally
  - Financially
  - Politically

Done correctly, they can optimize operations by:

- Sharing systems
- Joint purchasing
- Shared networks

[27] Cooperative Service through Consolidations, Mergers, and Contracts…Making the Pieces Fit. By: Chief Jack W. Snook and Chief Jeffrey D. Johnson. http://esci.us/resources/making-the-pieces-fit/ Last accessed 12/02/15

- Shared staff

The PSAP Optimization in the NG9-1-1 environment is expanded and included in Section 4 of this report.

5.4 PSAP Optimization Options

5.4.1 PSAP Operations Optimization

5.4.1.1 Basis for Operational Optimization

PSAPs often function as the emergency communications hub for the communities they serve. The critical goal of any optimization initiative is to further enhance public safety. As agencies open discussions regarding the potential for physical optimization, it is critical that operational expectations, such as expected service levels, are clearly identified.

The basis of PSAP optimization assumes that NG9-1-1 Core Services and the ESInet have been considered as discussed in this section of the report. Whether deployed at the County, Regional or State level, the NG9-1-1 environment provides PSAPs the flexibility to configure call flow and applications in a manner not previously available.

5.4.1.2 Optimized PSAP - Operational Models

In each model below, call handling is the common functionality. In a true NG9-1-1 deployment, it is not necessary for the CPE to be of the same manufacturer, and in larger deployments, e.g. regional or State, it is assumed that numerous CPE vendors will be in use.

5.4.1.2.1 Shared Services (Centralized)

A shared services center is where existing PSAPs centers are brought together under one roof or facility and possibly share management and resources. Several examples include Bexar Metro 9-1-1 District,[28] Licking County Regional Communications Center, Ohio,[29] and Bergen County Public Safety Operations, New Jersey.[30] A formal relationship is established through inter-local agreements, setting the entry and exit of agencies and the operational environment involved under the governing PSAP agency or authority. The public safety agencies themselves (law enforcement, fire, EMS) could operate as a combined entity, or individual separate entities. This model provides services for all public safety call intake and dispatching within the assigned area. Staff may utilize common technology, operational policies under a single form of governance.

Advantages:

- Common facilities provide the ability to share the benefits of common support services such as janitorial, food services, office supplies, and the support infrastructure.
- Takes advantage of common electrical, heating-ventilation-air conditioning (HVAC), and emergency power subsystems.
- The employees can be cross-trained and the schedules can be combined for added personnel efficiency.

[28] Buchholtz, B. (10/02/05). Email Interview.
[29] Carver, K. (10/27/15) Email Interview.
[30] DelVecchio F. (11/20/15) Email Interview.

- Creates an environment that is more flexible, and amplifies the commonalties in law, fire and medical dispatch.
- One operating environment for the consolidated 9-1-1 operations can optimize the use of computer aided dispatch (CAD), radio, mobile data, audio recorders, mapping, geographic information system (GIS, CPE and telephony systems) and Database Systems.

Challenges:

- Maintaining numerous Service Level Agreements (SLA's) for specific PSAPs may be challenging.
- Combining multiple agencies, which utilize different and incompatible computer systems into a multi-jurisdictional, multi-disciplinary, multi- agency, high-volume center can be difficult to implement and support.
- Bigger is not necessarily better if neither efficiency in service delivery nor economies of scale would result from consolidation of services.
- Emergency communications could be interrupted for all of the jurisdictions involved if proper attention is not given to redundancy and fallback planning.

5.4.1.2.2 Hybrid

This model can include variations wherein PSAPs maintain separate physical locations but share common call handling, and other services such as, radio, CAD or other public safety dispatching equipment over a secure managed network. These environments are positioned to readily move toward NG9-1-1 architectures.

An example of this model might be four local PSAPs sharing a common PSAP enterprise network, secondary network connectivity for redundancy, hosted CAD and CPE equipment. Additionally, radio technicians, system administrators, dispatchers and supervisors are able to assist each agency due to the common technology, applications, appliances and configuration of the hosted solutions and common technology platforms deployed among and between the PSAPs. Examples of this include Boulder County Regional PSAP and Upper Peninsula 9-1-1 Authority, Michigan. [31] [32]

Advantages:

- Local operational control, management and governance are maintained by each PSAP agency.
- The employees are cross-trained at the technical and operational level to assist each of the PSAPs.
- Common operating platforms and costs are shared among the PSAPs allowing the agencies the use of computer aided dispatch (CAD), radio, mobile data, audio recorders, mapping, geographic information system (GIS, CPE and telephony systems).
- Interoperability is increased with the use of common network and equipment so data and emergency calls can be transferred between the PSAPs.
- The design in itself is a disaster recovery design, allowing for primary PSAP personnel to easily move to a sister PSAP and continue operations.

[31] West, P. (12/05/05). Email Interview
[32] Johnson, G. (11/06/05). Email Interview.

Challenges:

- Where there is no regional 9-1-1 Authority, this model requires additional cooperation and trust among the agencies to manage global and agency configurations. For example, interfaces that rely on the PSAP and their sub agencies add complexity as equipment and appliances may be inconsistent across sub agencies or contract agencies.
- Difficult to implement and support if a common funding model is not established to share implementation and on-going support costs
- Requires PSAPs to collaborate, agree to modify operational policies, and spend additional time to gain consensus to move issues to conclusion that affect operations and technology implementation

5.4.1.2.3 Centralized Call Taking Center

In this model, 9-1-1 calls, which would normally be directed to individual PSAPs, are routed to a centralized call taking facility. These call takers perform immediate analysis and triage, then transfer the call to the appropriate law enforcement, or fire/ems agency of the jurisdictions involved for dispatch. They may also bridge multiple agencies together to respond to specific events or situations.

The dispatch agencies may share the same facility or be located at numerous geographic locations. Examples of this include Honolulu Police Dept. and Harris County 9-1-1 District, Texas. [33] [34]

All PSAP functions can remain the same.

Advantages:

- A large staffing base insures 9-1-1 calls are answered in a timely manner, potentially increasing service levels.
- Addresses local calling spikes, where a local PSAP may have required calls to queue prior to being sent to their designated 'overflow' PSAP.
- Provides a non-partisan call-taking environment.
- Regional call routing is simplified which could result in fewer call transfers.

Challenges:

- Requires a well-planned governance structure.
- Coordination and sharing of resources.
- Coming to a common ground on standard operating procedures can be difficult.
- Time is added to call processing.
- May be duplication of functions.
- Every Police/Fire/EMS call requires a transfer
- For very large call taking centers, appropriate geographic and tribal knowledge may not be available.

5.4.1.2.4 Consolidation by Discipline

This model keeps the existing PSAP structure in place, with law enforcement answering

[33] Burns, T. (10/02/05). Email Interview.
[34] Harris Info (11/01/05). Email Interview.

all 9-1-1 calls. However, Fire/EMS calls are transferred to a consolidated secondary PSAP. In this model, the secondary PSAP has the ability to dispatch Fire/EMS for all associated agencies. It provides for a higher level of specialization for both the Primary and Secondary staff. As an example, this model is currently being used successfully in one of the largest geographic Counties in the nation.

Advantages:

- Call takers are able to specialize in a specific discipline. As an example, dealing only with EMS types of calls. This may provide better quality of service to the public.
- Staffing provides the ability to handle 'surge capacity' or large call volume increases from a specific geographic area surrounding a single PSAP.
- Primary PSAPs will experience a decreased workload

Challenges:

- Every Fire/EMS call requires a transfer.
- Coming to a common ground on standard operating procedures can be difficult.
- Time is added to call processing.
- There is duplication of functions.

5.4.1.2.5 Virtual

This model requires shared infrastructure. The PSAP call handling equipment can be local or reside at a remote site or data center. An ESInet provides transport for the calls to be routed to numerous PSAPs. Provides for remote Session Initiation Protocol (SIP) positions anywhere.

Virtual environments can enable the use of shared PSAP subsystems such as CAD, Automatic Call Distribution (ACD), MIS, and mapping. Current examples of these include State of Maine 9-1-1 Program and Palm Beach County, Florida.[35] [36]

Advantages:

- Call routing is transparent to the 9-1-1 caller, regardless of location.
- The PSAPs can expand coverage areas and balance calls among sites.
- Good model for handling surge call volume.
- Each PSAP can still maintain its own local governance structure.
- Each PSAP can still choose local policy routing (e.g. ring all or ACD).
- Good model to support disaster recovery.
- This could be configured to enable multiple PSAPs to operate as one virtual call center.

Challenges:

- Requires detailed coordination between PSAPs.
- Appropriate operational structure (ex. Administration and support) needed to support the virtual environment.
- Local knowledge.
- Coordination and sharing of resources.

[35] Jacques, M. (09/23/05). Email Interview.
[36] Spalding, C. (10/07/05). Email Interview

- Coming to a common ground on standard operating procedures can be difficult.
- Requires ongoing cooperation and coordination of all participants.

5.4.2 Optimization Considerations and Factors

The goal of this section is to help the reader determine the PSAP optimization solution which best meets the unique needs of a given jurisdiction or area (local, county, region, state). Inherent in that process is the task of comparing the desired components of 9-1-1 service against the specific circumstances comprising a jurisdiction's needs. Each jurisdiction is unique and multiple technical and non-technical factors should be considered to work towards a final decision that is appropriate for a given community at a given time. The following reference documents provide optimization consideration factors:

- The Minnesota Governor's Work Group's "Public Safety Answering Point Consolidation: A Guidebook for Consolidation Strategies," states, "An overall improvement in the level of 9-1-1 answering and dispatch services provided to the community, participating agencies, and field personnel is the single most important reason to consider PSAP consolidation. "[37]
- An Oregon document, entitled, "Consolidation Analysis and Next Generation 9-1-1 Implementation Study" states, "9-1-1 Telecommunicators are truly the "first responder on the scene" and can substantially affect the outcome of an incident."[38]
- As California's 2010 Strategic Plan states, As stewards of the public trust, 9-1-1 public safety organizations have an obligation to enhance internal capability and autonomy through the retention of adequate resources, skilled personnel, technological capability, and authority to execute all aspects of the 9-1-1 Program."[39]

The following section of this document is not exhaustive, but includes issues that authorities/agencies may wish to consider as part of the overall process of determining the optimal 9-1-1 solution in relation to the specific circumstances in the community they serve.

This process has two assumptions:

1. Primary objective is meeting the needs of 9-1-1 callers by improving the capabilities and quality of 9-1-1 answering and dispatch services.
2. Secondary objective is providing necessary resources for the 9-1-1 Telecommunicator, previously defined as a "person employed by a PSAP and/or an Emergency Medical Dispatch (EMD) Service Provider qualified to answer incoming

[37] Minnesota Governors Work Group "Public Safety Answering Point Consolidation: A Guidebook for Consolidation Strategies, "An overall improvement in the level of 9-1-1 answering and dispatch services provided to the community, participating agencies, and field personnel is the single most important reason to consider PSAP consolidation."

[38] "State of Oregon Office of Emergency Management, Consolidation Analysis and Next Generation 9-1-1 Implementation Study": http://www.oregon.gov/OMD/OEM/or9-1-1/docs/kimball_consolidation_analysis_next_gen_implementation_study.pdf Last accessed December 4, 2015.

[39] California Office of Emergency Services, California 9-1-1 Strategic Plan (2010), http://www.caloes.ca.gov/for-businesses-organizations/plan-prepare/ca-9-1-1-information, last accessed September 3, 2015.

> emergency telephone calls and/or provides for the appropriate emergency response either directly or through communication with the appropriate PSAP."[40]

5.4.2.1 Operational Considerations

Technical, administrative, and financial issues, as identified in this report, are important considerations in evaluating the potential of sharing resources, but of equal importance, are operational considerations. Deciding exactly what resources will be shared and how the work of PSAPs will utilize the shared resources has important implications for exactly how the public's need for 9-1-1 service will be met. It will also directly affect the Telecommunicators who are held responsible for handling 9-1-1 calls from the community.

The PSAP operations have historically been unique to each PSAP, and driven by the needs of the agencies they serve and the individual agencies actively participate in defining the operational procedures specific to that agency. The more agencies served by a single PSAP the more complex the operational procedures become. However, it is important to note that as NG9-1-1 efficiencies are gained with optimized networks and core services, the melding of standardized operating procedures will need to be accomplished. Through cooperation and partnerships with multiple agencies a detailed comparison of existing policies and procedures will be required, as well as careful consideration should be given to how all changes could affect PSAP service requirements. Part of this comparison must include examination of the roles and responsibilities of the Telecommunicator, and modify roles, where appropriate, to ensure the successful fulfillment of their assigned duties.

9-1-1 Jurisdictions currently have procedures and processes in place to deploy, manage and maintain E9-1-1 systems, and their interactions with vendors, especially a 9-1-1 service provider. As PSAPs migrate to NG9-1-1 those procedures and processes may need to evolve to support the next generation environment.

The NENA's NG9-1-1 Transition Planning Considerations Committee produced the "NENA NG9-1-1 Transition Plan Considerations Information Document" which addresses technical and limited data transition elements (based on originating and terminating entities as they progress from legacy to NG9-1-1 environments).[41] However, the PSAP operational impacts associated with NG9-1-1 warrant similar attention. As noted by NENA NG9-1-1 Planning document,

> *The transition to NG9-1-1 has impacts upon operations within all stakeholder organizations. The level of impact may depend upon the responsibility of the entity processing the emergency call. For example, for entities in originating networks it may be as simple as redirecting calls to the NG9-1-1 network. For entities such as 9-1-1 Authorities it may require developing transition plans to upgrade or replace equipment, and to cope with the databases that support the NG9-1-1 services and capabilities. It is expected that NENA's Committees will continue to develop operational standards that will facilitate the introduction of NG9-1-1.*

[40] National Emergency Number Association, NENA Master Glossary of 9-1-1 Terminology, http://www.nena.org/?page=Glossary Last accessed December 2, 2015.
[41] NENA NG9-1-1 Planning Document: http://www.nena.org/?page=ng9-1-1planning Last accessed December 2, 2015.

At the publication of this report NENA, officially initiated the development of *Operations, Monitoring and* Managing *NG9-1-1 Systems* document and interested parties should monitor the NENA website for publication of this guide.

5.4.2.2 Organizational Operation

In the legacy 9-1-1 environments, public safety agencies have had the luxury to operate in silos. Local police, fire and EMS agencies have designed their responses to fit local needs. In general, agencies expect their PSAPs to dispatch them to a finite level. Each entity being able to individualize the way they respond to specific call types with a much-localized fit. As NG9-1-1 becomes a reality, it will allow PSAPs the capability to dynamically utilize partner PSAPs to assist during heavy call traffic situations and/or outages. During those times, 9-1-1 Authorities will need to work out how first responders will receive the call for them to respond to. As PSAPs must cooperate and collaborate call answering, call entry and call delivery, it will be imperative that local public safety agencies begin to cooperate and collaborate to design local responses to be as like as possible to the extent possible. The TFOPA recommends that local and regional PSAPs begin partnerships and collaborations for the planning, implementation and operations of NG9-1-1 systems.

At the organizational level, it will be important to come to agreement on the desired outcomes for operational consideration and specific actions for reaching those outcomes. The priorities of each individual agency must be considered, and collective goals made for providing 9-1-1 services. Discussion and decision may include such varied topics as:

- Establishment of Multi-Jurisdictional Operations Planning Committee (Policy, operational procedures and cross-jurisdictional boundary issues)
- Personnel Operational Issues (i.e. Salaries, Benefits, Code of Conduct, etc.)
- Labor Laws / Labor Contracts
- Services Provided (e.g. EMD, Police, Fire Dispatch, Poison Control, Language Line)
- Operational Politics
- Desired method of operation[42]
- Desired level of efficiency
- Required level of business continuity
- Load sharing
- Framework for cooperative decisions
- Quality Assurance (QA) / Quality Control (QC)
- Security – physical and cybersecurity
- Differences in CAD, phone, radio, recording equipment, GIS
- Existing processes for budgeting, accounting, payroll
- Accreditations and certifications
- Disaster Recovery

[42] Recommended Call Processing Standards currently exists with the National Emergency Number Association, APCO International and the National Fire Protection Association. At the publishing of this document NENA was reviewing, updating and consolidating a recommended standard covering the following NENA documents:
56-001 Guidelines for Minimum Response to Wireless 9-1-1 Calls
56-005 Call Answering Standard / Model Recommendation
56-006 Emergency Call Processing Protocol Standard
56-501 Silent or Hang-Up 9-1-1 Calls for Service Information Document

- Continuity of Operations plans
- Plans for deploying advancing technology
- Managing relationships with carriers and emergency responders

All operational functions should be accounted for and agreed upon as part of any resource sharing agreement.

The largest ongoing investment most PSAPs make is in personnel, and multiple publicly available reports cite personnel as the largest cost for PSAPs. It is the responsibility of the agency that employs Telecommunicators to ensure that they have the tools to succeed in answering and processing 9-1-1 calls. Sharing services among PSAPs not only requires technical, administrative and financial arrangements, but must also include issues related to staffing, such as:

- Discrepancies in policies and standard operating procedures
- Variances in job descriptions (including non-9-1-1 duties), hiring practices, pay, scheduling, supervision, seniority, benefits and other HR issues (e.g., reward and discipline procedures)
- Inconsistencies in staffing levels
- Addressing staffing issues related to fatigue. As with other "shift" workers, shift rotations of the Telecommunicator require proper planning to minimize the health effects of the 24 hours operation. Staffing resources are available that incorporate appropriate measures, and jurisdictions are encouraged to include such ideas when considering how to combine staffing.[43]

5.4.2.3 Training and Support

The training provided to Telecommunicators varies widely among PSAPs. Comparison of existing training requirements among PSAPs may reveal gaps or inconsistencies that must be addressed to ensure seamless provision of shared services.

Combining training for multiple PSAPs may increase efficiency. When each PSAP is no longer exclusively responsible for its own training, it becomes possible to share training sessions and provide coverage for each other's training sessions. Standardized training offers the option of load sharing and the possibility of covering for each other's PSAP, if staffing needs suddenly increase. In order to enjoy these benefits, plans must be developed and executed that address and include:

- An agreed upon method of operation
  - Desired levels of efficiency
  - Load sharing
- Differences on job descriptions (i.e., call processing, dispatching)
- Discrepancies in CAD systems
- Inconsistencies in standard operating procedures
- Variances in training and how they will be addressed.

In addition to the items above, there should be consideration and focus given to emotional and quality of life issues. PSAP consolidation represents change for existing PSAP employees and stakeholders and may require difficult adjustments. Managing this change is

[43] http://www.cdc.gov/niosh/docs/97-145/pdfs/97-145.pdf, Last accessed December 2, 2015

critical to the success of any resource sharing effort. Change management methods, including the active involvement of staff may be key in successful transition. There will be a need to provide a steady stream of updates and accurate information as deliberations occur, and if decisions are made and implemented.

Additional and enhanced data that will also be provided via the 9-1-1 caller will requirement management oversight and additional operational procedures. At the publication of this report, an Operations Monitoring and Managing of NG9-1-1 was in development by NENA.

There is widespread acceptance of the fact that the job of the 9-1-1 Telecommunicator is stressful.[44] Telecommunicators are expected to process calls where terrible events have occurred. But repeated exposure can take its toll. And a study by researchers at Northern Illinois University suggests that the Telecommunicators are at risk for developing symptoms of Post-Traumatic Stress Disorder (PTSD). Researchers analyzed the responses of almost 200 experienced (averaged more than 10 years) emergency dispatchers from 24 states and found almost five percent reported symptoms severe enough to qualify for a diagnosis of PTSD.[45]

Managing any additional stress brought on by organizational change will be important to the success of any efforts to share resources, whether the shared resources are virtual or physical. Taking the opportunity to address stress for Telecommunicators may have a positive effect on job satisfaction, performance, and retention. There are resources available that employ effective methods for dealing with stress and PTSD symptoms, that allow the Telecommunicator to stay on the job and will allow the PSAP to benefit from the expertise gained from successful handling of difficult situations.[46] Incorporating the availability of stress resources within the context of managing change could be an important way of demonstrating the value of staff to the organization, and a worthy investment.

5.4.3 PSAP Infrastructure Architecture Deployment Optimization Models

Whereas other sections described NG9-1-1 PSAP optimization from a governance and operational perspective, this section describes the PSAP infrastructure architecture models that enable the efficient sharing of hardware within a single PSAP, or the efficient sharing of both hardware and software services across multiple PSAPs. These architectural models for sharing infrastructure and software services have become prevalent in commercial and enterprise markets and can be applied to future NG9-1-1 deployments.

These infrastructure deployment models configured to support each of the operational models discussed previously, thus allowing PSAPs Telecommunicators in diverse physical locations to function in a coordinated manner as a virtual PSAP environment, or in a more traditional multi-PSAP environment with separate jurisdictional/ administrative domains.

Further these deployment models can be implemented independently at the level of individual services, such as call taking or CAD, or in combination if there is a desire on the part of those deploying these solutions that some services be shared while others are not. Finally,

---

[44] Gouveia, A. (2013). The Top 10 Most Stressful Jobs Find Out Which Careers Come with the Most Worry. http://www.salary.com/the-top-10-most-stressful-jobs/slide/5/ Last accessed August 8, 2015

[45] Northern Illinois University, NIU researchers find link between 9-1-1 dispatchers, PTSD symptoms, s/news/2012/03/9-1-1-ptsd.shtml" http://www.niu.edu/mediarelations/news/2012/03/9-1-1-ptsd.shtml, Last accessed August 8, 2015.

[46] 9-1-1 Wellness Foundation, Building Your Stress Program, .com/building-your-psap-csmp/" http://9-1-1wellness.com/building-your-psap-csmp/ last accessed August 8, 2015.

these models can be deployed at any scale required, including at the local, regional or state level. Therefore, rather than describe every permutation of potential deployment models, this section will focus on the high level models themselves.

Additionally, these PSAP infrastructure deployment models offer PSAPs flexible purchase, implementation, operation and maintenance, and service options, which allow jurisdictions to implement the appropriate level of optimization, based on their needs. To fully understand the shared infrastructure architecture models the Task Force has also provided a discussion of the On-Premise Dedicated Infrastructure model for comparison purposes.

The NG9-1-1 PSAP architecture optimization will build upon the use of several. by now, widely deployed enterprise technologies that make up the core of modern computing and communications systems and which PSAPs will start to utilize even more extensively than they do today as they transition to NG9-1-1 systems. These technologies form the foundation for next generation infrastructure deployments across all industries, and not just in NG9-1-1.

- **Internet Protocol (IP):** Internet Protocol-based networking is foundational to NG9-1-1, the ESInet WAN and PSAP LAN. The multimedia capability, interoperability, scalability and robustness of the technology that underlies the Internet are leveraged in NG9-1-1 by the use of IP-based networks and communications systems.
- **Client-Server:** Modern data processing and communication systems utilize this model in which client software deployed at the user end point (in the public safety context, usually at a PSAP Telecommunicator position) works in conjunction with server software deployed in an on-premise data equipment room or a shared infrastructure data center. The server-side implementation of client-server deployment is typically called a software service.
- **Server Virtualization** Software technologies, including virtual machine and emerging container technologies, that allow multiple applications to share a common server hardware and storage platform.
- **Cloud** Virtualization technology taken to a larger scale where virtual machines / containers can be created for software services in an on-demand fashion using a private government intranet infrastructure or an internet-accessible public infrastructure of computing hardware and storage; cloud technology improves infrastructure usage efficiency and service reliability and provides elasticity to support peak demands on resources.

The following subsections will describe the various types of PSAP architecture deployment models and their relative impact on specific optimization factors. The models described are those envisioned as potential "real world" PSAP deployments.

This section is related to technical architecture, and will not address some of the political factors such as governance, joint service agreements, cost and operational allocations to jurisdictions, and legal considerations. Those factors are described in other sections. However, these architecture models do significantly impact specific relevant optimization factors that can in turn be qualitatively compared and contrasted in terms of their relative value for each model.

Key optimization factors that should be included in a jurisdiction's consideration of the optimization models include but may not be limited to:

- Financial
  - Solution costs (e.g., equipment, capital expenditure/operational expense)
- Interoperability

  - Functional interoperability
  - Geographic interoperability: local, county, multi-county, state, national
  - Data sharing
- Survivability/Reliability (operational)
  - Level of service redundancy
  - Level of geo-diversity
- Elasticity/ Scalability
  - Ability to adapt to unanticipated peak loads
  - Ability to bring on additional jurisdictions without re-architecting
- Security
  - Information Security
  - Cyber-attack resiliency
- Operational Staffing
  - Technical Support

5.4.4 NG9-1-1 PSAP Functional Elements

Next Generation 9-1-1 PSAPs will benefit from several new capabilities that will provide greater insight into the nature of each caller's emergency and will help guide Telecommunicators on the most effective response that should be dispatched. Further discussion is needed in reference to applications, interfaces, and services expected to be available in NG-9-1-1. While referenced below, this document does not go into detail on each.

The NG9-1-1 PSAP infrastructure elements, many of which carry-over as expected from legacy PSAP operations, may include but is not limited to the following:

- 9-1-1 Call-taking (Voice, Text, Data, Images, Video)
- Management Information System (MIS) and Analytics
- Incident recording (Multimedia - Voice, Text, Data, Images, Video)
- Geographic Information Systems (GIS)
- Computer Aided Dispatching (CAD)
- Records Management Systems (RMS)
- Data Retention/Records maintenance
- Addressing- Automatic Number Identification (ANI) Automatic Location Identification (ALI) services
- Advanced Services & Applications
  - Criminal Justice Information Database Access
  - Emergency Medical Dispatch (EMD)
  - Social Media Mining
  - Social Media External Communications
  - Internet of Things (IoT) Ingest
  - Data Analytics (Descriptive, Predictive, Prescriptive)
  - Video Surveillance
  - Media Analytics (Video, Audio)
  - Situational Awareness
  - Analytics Visualizations
  - Others

- Location Validation Function (LVF)[47]

5.4.5 NG9-1-1 Architecture Deployment Models

5.4.5.1 Dedicated Infrastructure Architecture Model

5.4.5.1.1 On-Premise Dedicated Infrastructure Architecture Model

This model has been used universally in the past, and is still used by the vast majority of PSAPs. Premise-based deployments are characterized by having all clients and required servers collocated at a single physical facility. This architecture is applicable to a single jurisdiction that wants to more effectively utilize server and storage hardware across a single PSAP's functional elements (Call-taking, CAD, RMS, etc.). In this configuration, there is no sharing of resources outside of the PSAP or command center in question.

5.4.5.1.1.1 Options

5.4.5.1.1.2 Implementation Options

- Geo-diversity
- Virtualization

5.4.5.1.1.3 Financial Acquisition Options

- Non-Recurring Cost/ Capital Expenditure (CAPEX)
- Recurring Cost/Operating Expenditure (OPEX)
- Combination of the above

5.4.5.1.1.4 Network Options

- Government owned and managed
- Vendor owned and managed
- Combination of the above

5.4.5.1.1.5 System Maintenance

- Government operated and managed
- Vendor operated and managed
  - Software as a Service
  - Infrastructure as a Service
- Combination of the above

Figure 5-3 is a pictorial representation of this architecture model.

[47] LVF is a NG9-1-1 core service that can be collocated with other NG9-1-1 core services or with the PSAP infrastructure elements.

On Premise Dedicated Infrastructure Architecture Model

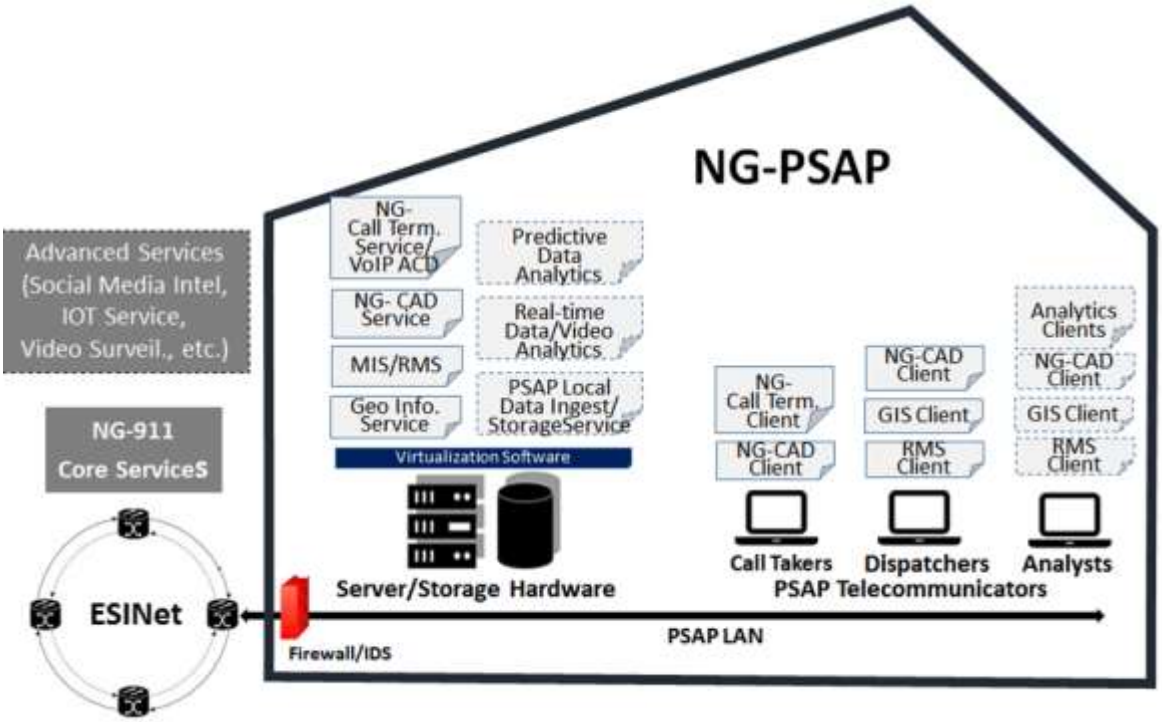


Figure 5-3: On-Premise Dedicated Infrastructure Architecture Model Example

Advantages

- Political – Same as what is done today
- Governance – Relatively straightforward, maps to what is deployed today; each PSAP uses its own governance model
- Security – Relatively secure
- Operational – Same as what exists today; requires no real additional effort

Challenges

- Financial – May be the most expensive option as backroom hardware and related services are duplicated in every PSAP. To verify or validate this, further study may be warranted
- Interoperability– Is inherently the least interoperable option; by definition standalone unless specific effort is made to interconnect "islands" of capability at each individual PSAP
- Survivability – Is inherently the least survivable option

5.4.6 Shared Infrastructure Architecture Model

The shared infrastructure model enables multiple PSAPs to share the NG9-1-1 PSAP functional infrastructure elements that meet the needs of individual PSAPs or other jurisdictional entities fielding a system. This shared infrastructure deployment model enables multiple PSAPs (multiple tenants) to share the server-side components of NG9-1-1 PSAP functional infrastructure elements within either one of the PSAP facilities (on-premise shared infrastructure), or in a shared data center facility (data center hosted, shared infrastructure). This model can retain independent client-side deployments at the respective PSAP facilities housing

the telecommunicators.

5.4.6.1 On-Premise Shared Infrastructure Architecture Model

In an on-premise shared infrastructure deployment model, the server-based hardware and storage components providing required PSAP functionality are located in PSAPs and shared by multiple PSAPs.

5.4.6.1.1 Options

5.4.6.1.1.1 Implementation Options

- Geo-diversity
- Virtualization

5.4.6.1.2 Financial Acquisition Options

- Non-Recurring Cost/CAPEX
- Recurring Cost/OPEX
  - Software as a Service (SaaS)
  - Infrastructure as a Service (IaaS)
- Combination of the above

5.4.6.1.3 Network Options

- Government owned and managed
- Vendor owned and managed
- Combination of the above

5.4.6.1.4 System Maintenance

- Government operated and managed
- Vendor operated and managed
  - Software as a Service (SaaS)
  - Infrastructure as a Service (IaaS)
- Combination of the above

5.4.6.2 Hosted, Shared Infrastructure Architecture Model

In a data center hosted, shared infrastructure deployment model, the server-based hardware and storage components providing required PSAP functionality are "hosted," in a data center and shared by multiple PSAPs. In an on-premise shared infrastructure deployment model, the server-based hardware and storage components providing required PSAP functionality are located in PSAPs and shared by multiple PSAPs.

The PSAP facilities require client software on a PC, laptop, or tablet at their operator positions to access these shared services. In this model, PSAP administrators can retain the use of local Telecommunicators, and in fact these individuals can be deployed anywhere that has network access connectivity back to the shared data center or to the PSAP facility hosting the shared infrastructure.

5.4.6.2.1 Options

5.4.6.2.1.1 Implementation Options

- Geo-diversity
- Virtualization

5.4.6.2.1.2 Financial Acquisition Options

- Non-Recurring Cost/CAPEX
- Recurring Cost/OPEX
  - Software as a Service (SaaS)
  - Infrastructure as a Service (IaaS)
- Combination of the above

5.4.6.2.1.3 Network Options

- Government owned and managed
- Vendor owned and managed
- Combination of the above

5.4.6.2.1.4 Data Center Options

- Government owned and managed
- Vendor owned and managed
- Combination of the above

5.4.6.2.1.5 System Maintenance

- Government operated and managed
- Vendor operated and managed
  - Software as a Service (SaaS)
  - Infrastructure as a Service (IaaS)
- Combination of the above

Figure 5-4 is a pictorial representation of this deployment model.

Sample Hosted, Shared Infrastructure Architecture Model

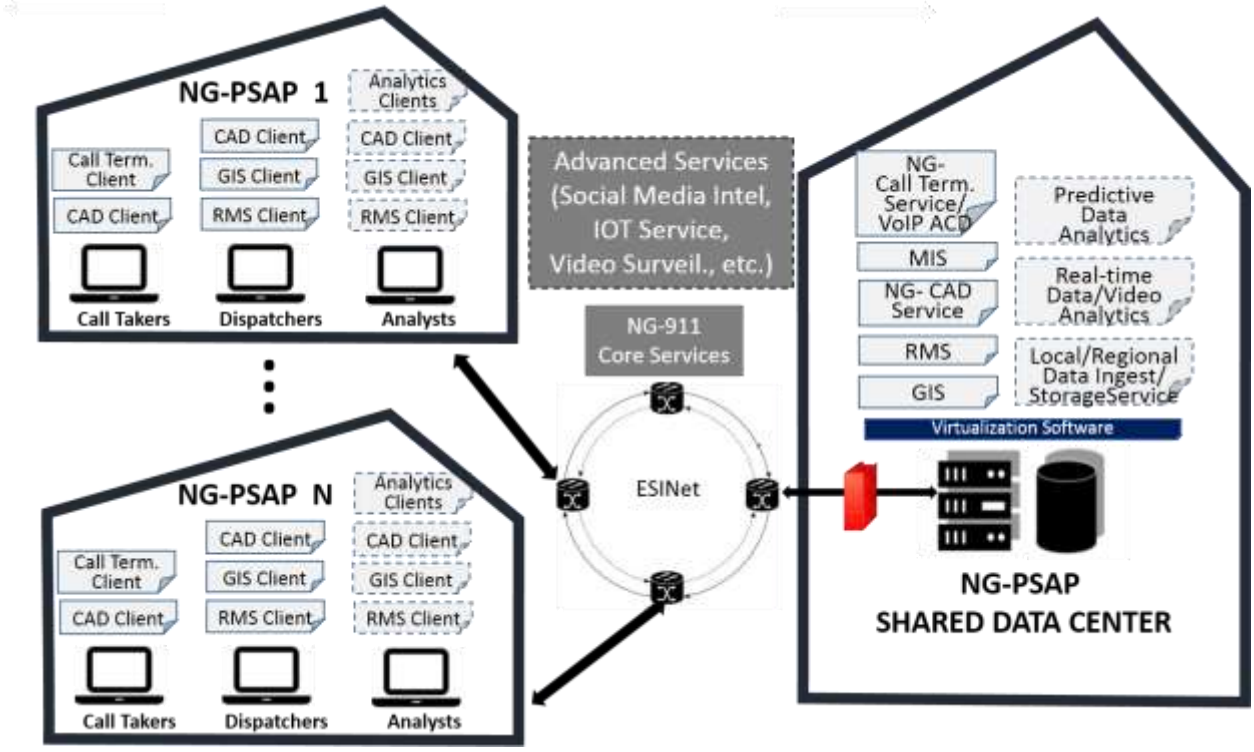


Figure 5-4

Advantages

- Interoperability – Inherent in system architecture and relatively easy to setup between PSAPs
- Financial – Shared infrastructure resources reduces overall cost of system and allows that cost to be shared
- Survivability – automatic failover and geo-diversity options are typically inherent in system architecture; higher survivability in terms of 9-1-1 service provision

Challenges

- Governance – Independent PSAP governance is no longer an option and therefore work must be done to develop a joint governance model
- Political will – In a fully shared infrastructure model, all but a single PSAP, or potentially none, will retain a "full system". Most will be using only clients to connect to the shared infrastructure services. Potential "loss of prestige"
- Operational – Like governance, will require some effort to create a joint operational model, something that does not already exist in all areas

5.4.6.3 Hybrid – Dedicated / Shared Infrastructure Architecture Model

In a Hybrid Dedicated & Shared Infrastructure Architecture, server-based hardware and storage components providing required PSAP functionality are deployed in a combination of

both on-premise dedicated and shared infrastructure as required and appropriate. This model allows administrators to share certain PSAP infrastructure and functions (such as call processing and mapping) while maintaining dedicated infrastructure for other functions (such as CAD, RMS and incident recording). When assessing this model one must keep in mind that the advantages associated with infrastructure sharing only apply to those infrastructure services and functions that are shared. Figure 4-3 is a pictorial representation of this specific architecture deployment, which is only one of many potential examples of combining dedicated on-premise and shared services.

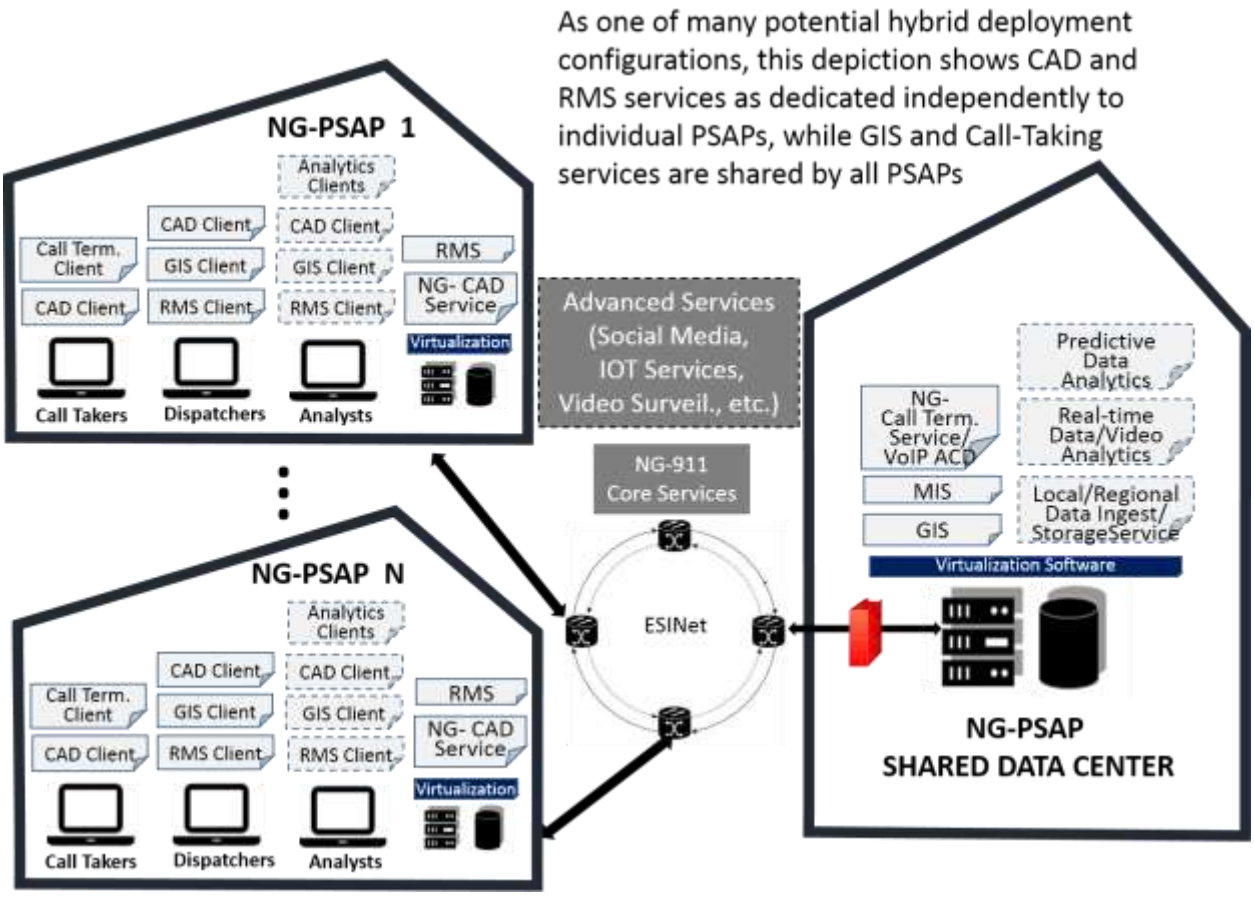


Figure 5-5

5.4.6.3.1 Options

5.4.6.3.1.1 Implementation Options

- Geo-diversity
- Virtualization

5.4.6.3.1.2 Financial Acquisition Options

- Non-Recurring Cost/CAPEX
- Recurring Cost/OPEX
  - Software as a Service (SaaS)
  - Infrastructure as a Service (IaaS)

- Combination of the above

5.4.6.3.1.3 Network Options

- Government owned and managed
- Vendor owned and managed
- Combination of the above

5.4.6.3.1.4 Data Center Options

- Government owned and managed
- Vendor owned and managed
- Combination of the above

5.4.6.3.1.5 System Maintenance

- Government operated and managed
- Vendor operated and managed
  - Software as a Service (SaaS)
  - Infrastructure as a Service (IaaS)
- Combination of the above

5.5 ESInet Optimization Considerations and Factors

5.5.1 ESInet Architecture

Today, ESInet Architectures are following an evolutionary model. IP network capabilities are deployed based on Public Safety needs and readiness to implement NG9-1-1 services. The ESInets deployed today are primarily used for delivery of limited NG9-1-1 Services such as legacy Selective Router and ALI replacement. As such, all external interfaces, or demarcation points, are well defined, limited in scope and well controlled. This limited ESInet Architecture norm will change as the NENA i3 vision is realized with Originating Service Providers (OSPs) providing data feeds, enhanced service providers establish interconnections with ESInets across the United States and ESInets become interconnected. The Economics, including funding, is a challenge in this changing environment as legacy conventions are challenged and Public Safety Authorities work towards providing new emergency services capabilities.

Over time, ESInet Architectures will become more complex to design, manage, secure and evolve. As a rule, ESInets should be modular in nature, evolution and change is expected. ESInet architectures are explained in the NENA document 08-506 “Emergency Services IP Network Design”. The ESInet definition from NENA 08-506 is as follows:

> *An ESInet is a managed IP network that is used for emergency services communications, and which can be shared by all public safety agencies. It provides the IP transport infrastructure upon which independent application platforms and core functional processes can be deployed, including, but not restricted to, those necessary for providing NG9-1-1 services. ESInets may be constructed from a mix of dedicated and shared facilities. ESInets may be interconnected at local, regional, state, federal, national and international levels to form an IP-based inter-network (network of networks).*

The ESInets consist of the following categories of capabilities. For the purposes of ESInet

discussions and brevity, these categories are abstracted from generally accepted networking models.

- Transport
- Internet Protocol (IP) Services
- Management Infrastructure
- Security Infrastructure

5.5.1.1 Transport

Transport provides the physical medium to move IP packets within an ESInet and establish interface points with external entities. Transport includes physical conduits and IP equipment, such as routers and switches. Common circuit types for ESInets are MPLS, Fiber, Sonet, Metro Ethernet, T1/DS3, Microwave and 3G/4G wireless. It is likely, ESInets may be constructed from a mix of dedicated and shared transport facilities. Transport for an ESInet may be purchased from a bandwidth provider or utilize a network of the Public Safety entity or its associated government establishment. Regardless, the business model to establish the transport, the network and facilities must meet "Public Safety Grade". The provider of the Transport must be aware of the emergency services requirements for redundancy, availability, performance and management. Including specific rules such as FCC *Report and Order* 13-158 "…to improve the reliability and resiliency of 9-1-1 communications networks…" Providers must implement management processes capable of meeting emergency services criteria, including 99.999% availability that is just under 5 minutes 16 seconds of unscheduled downtime per year. Bandwidth strategies must consider current needs, economics of bandwidth available products and expandability to future needs.

An ESInet has the following interfaces with corresponding points of demarcation. Demarcation points, or the interface where formal change of oversight responsibility is differentiated between two parties, are usually a port on an interface device, such as a router, SBC, Firewall, or a TDM port card. An ESInet has, or can have, the following interfaces types:

- Originating Service Providers (OSPs)
- PSAP Customer Premise/Processing Equipment (CPE)
- Legacy Selective Routers
- Other ESInets
- FirstNet (future)
- Emergency Communications Cybersecurity Center (future)
- Provisioning interfaces
- Management interfaces
- Supplemental Services (e.g., Additional Data Services)
- The Public Internet (NOT RECOMMENDED)

5.5.1.2 Internet Protocol (IP) Services

Internet Protocol (IP) Services includes IP Addressing and Dynamic Routing Protocols. Quality of Service (QOS) mechanisms must be implemented to ensure critical 9-1-1 services are not impacted by other services provided on the ESInet. The ESInets are complex IP networks that are evolving and will become ever more complex as more capabilities are provided and more entities participate in providing features. The ESInet requires an experienced authority to

manage Internet Protocol Services to performance, reliability, redundancy and security requirements. An additional set of routers and switches may be present for IP Services, especially if the Transport network provider is a different entity from the ESInet Service Authority. A private Directory Name Service (DNS) is expected to exist within each ESInet. IP Addressing is managed within well-controlled and defined addressing domains that also map to the security strategy. Addressing is specific to each solution domain and all interfaces are well defined and managed. An open interface to the public "Internet" should not be allowed.

5.5.1.3 Management Infrastructure

Management infrastructure provides the overall framework for provisioning, monitoring, reporting and maintaining the ESInet. Provisioning functions exist for the ESInet itself and for the services that are built upon the ESInet. Network Operations Centers (NOCs) are key elements of an ESInet management infrastructure. There will usually be multiple NOCs involved, considering Transport services, ESInet management and the services that reside upon the ESInet. Management of the ESInet should consider the operational risks that are introduced in a dynamic and changing operating environment. Coordination of management functions to maintain expected services quality is a significant endeavor.

5.5.1.4 Security Infrastructure

Security Infrastructure includes appliances and practices to secure, monitor, detect intrusions, authenticate users, mitigate events and recover. The ESInet provides a foundation of security capabilities to protect the ESInet itself and the services that reside upon the ESInet. Border Control Functions (BCF) functions, including Sessions Border Controllers (SBCs) and Firewalls are used to secure interface demarcation points. Security concepts and capabilities are discussed in Security "NENA 75-001 Security for Next-Generation 9-1-1 Standard (NG-SEC)". Again, security is present at many levels and involves all entities that are providing services and capabilities to the ESInet and the services that reside upon the ESInet. The Security requirements and practices are touched on here to identify their need and emphasize their importance as an integral ESInet design consideration. However, they are more thoroughly addressed within the TFOPA WG-1 report focused on Cybersecurity.

5.5.2 Defined Uses & Configurations

As with traditional IP networks, there is no single definition or configuration that can be used to summarize all possible ESInets. Rather, several use cases are presented to define the configurations that are representative of the majority of ESInets uses envisioned. It must be recognized that specific local, regional, or state requirements for ESInets will vary widely; therefore the following use cases are presented from a macro perspective. These use cases define a framework definition for functionality that an ESInet is intended to provide, but it is also instructive to define what an ESInet is not intended to provide as well.

Today many agencies have a variety of IP networks within their facilities and jurisdictions. Within the PSAP environment many IP networks are "walled gardens" and typically serve a specific application. [48] For example, many call handling platforms rely on a

[48] A "walled garden" refers to an environment where users and applications are restricted to certain content and connectivity and are allowed to access specific, limited portions of the local network. The main purpose of creating a walled garden is to shield users, applications, and network devices and to

walled-garden network to provide connectivity between telephony workstations and servers at the premise, but have limited or no connectivity to other networks. Similar configurations are common within radio communications console environments and computer aided dispatch networks.

The use of walled-garden environments was a chosen and acceptable architecture in the past, as there were limited use cases for interconnectivity among disparate networks. In addition, application vendors preferred walled gardens due to their high degree of security and control. The convergence of applications and the ever-increasing case for data sharing have drastically diminished the usefulness and applicability of the walled garden architecture. Connectivity between networks is now more the norm than the exception.

Connectivity between emergency services application networks, however, does not necessarily create an ESInet. The interconnection between a telephony network and a radio or computer aided dispatch network, for example, does not in and of itself create an ESInet. Emergency services applications that may transit an agency, jurisdictional, or regional intranet similarly do not create an ESInet.

As defined, an ESInet must provide, "…the IP transport infrastructure upon which independent application platforms *and core functional processes* can be deployed, *including*, but not restricted to, those necessary for providing NG9-1-1 services [emphasis added]."

The end-state of a fully NG9-1-1 environment is a network of networks. Optimization results from scale. Optimal configurations will result from ESInets that are designed and deployed to serve populations that maximize the utilization of the networks and meet the needs of the served Public Safety Authorities.

The following use cases do not distinguish who operates and maintains the ESInet IP transport elements. An entity may choose to operate their own IP transport or contract for those services. In most cases IP transport is procured from IP transport providers, but all or local, regional or state funded multi-purpose IP networks may provide part of the IP transport services. 9-1-1 Jurisdictions utilizing multi-purpose IP transport networks for 9-1-1 call traffic must be aware of the special requirements placed on emergency services network functions. These include:

- Availability of infrastructure elements and the overall service
- Identification / tagging of infrastructure elements to ensure appropriate protections and handling.
- Management life cycle – End-of-Life product cycles must be managed
- Critical timeframes – 9-1-1 calls volume periods should be considered when planning and performing maintenance events.
- Quality of Service (QOS) – 9-1-1 functions must be given priority over other functions/services utilizing the network and 9-1-1 calls and call setup times must not be impacted.

In all cases where a 9-1-1 Authority is procuring products and services, there will be contract management oversight responsibilities.

create a quarantined environment that is difficult to infiltrate.

5.5.2.1 Use Case: Local ESInet

This use case defines a configuration in which the local authority elects to host Next Generation Core Services (NGCS) within existing PSAP datacenters or facilities and maintains their own ESInet. For this use case the agency or authority maintains robust, reliable facilities within which the NGCS are hosted.

The authority either provides or sub-contracts management functions to provide public-safety grade reliability and uptime of 99.999% or greater. Given the complexity of managing a network of this type – one that provides NGCS to a local area– and the resources required to maintain the network, this is likely the least common type of deployment.

Advantages:

- Local Control of platform and applications
- Establish as initial or "seed" ESInet that may expand to include other 9-1-1 Authorities to become a shared ESInet

Challenges:

- Cost of dedicated platforms and redundancy
- Difficulty of staffing/retention of Subject Matter Expert (SME) knowledge within local area
- Does not achieve any economies of scale for investment or staff

5.5.2.2 Use Case: Shared-Hosted ESInet

This use case defines a configuration in which a regional entity authority (group of PSAPs, county, multiple counties or state) elects to host Next Generation Core Services (NGCS) on a shared ESInet. This use case is optimized through economies of scale, either by maximizing the number of agencies served, or by optimizing the number of calls processed by the infrastructure, or by serving a large geographic region.

The authority either provides or sub-contracts management functions to provide public-safety grade reliability and uptime of 99.999% or greater.

Advantages:

- Regional Control of platform and applications
- Dedicated Resources – should reach an economy where resources can be dedicated but may need some subcontract work to maintain expertise and sufficient staff for vacation coverage.

Challenges:

- Cost of dedicated platforms and redundancy if not sufficient scale to realize efficiencies.
- Depending on deployment size, may not achieve any economies of scale for investment or staff
- Difficulty of staffing/retention of SME knowledge within area, depending on scale of deployment or authority.

5.5.2.3 "Hybrid" ESInet

This use case defines a configuration where some elements of the Shared Hosted ESInet are combined with elements that are contracted. For example, a 9-1-1 Authority may provide their own "dark fiber" network facilities and contract a service provider to build and manage the IP network services ride upon those network facilities.

Advantages:

- Greater control of specific network elements
- Potential for greater redundancy
- Leverage existing facilities, resources and capabilities where they exist and supplement only those specific elements that don't

Challenges:

- Potentially greater capital expenditures
- Increased management & administration requirements to integrate disparate elements
- Additional effort to identify facilities, resources and capabilities that can meet requirements.

5.5.2.4 Use Case: Contracted, Managed ESInet

This use case defines both the most basic and most prevalent type of ESInet deployment at the time of this document. This is a "shared" network between multiple served PSAP tenants, which could scale from small region to nationwide. The managed service vendor builds and maintains the ESInet. The PSAPs served by this infrastructure could be geographically near or distant from each other. This model assumes that the 9-1-1 Authority does not operate the ESInet themselves but that all operational and management functions are performed by the hosting service.

This type of ESInet does not necessarily connect directly to the PSAP premise, but could provide terminating circuits to the PSAP CPE in a hosted location. A hosted PSAP CPE model may serve multiple PSAPs in a multi-tenant fashion. In the case of call handling equipment that is hosted within the ESInet, the only connectivity from the ESInet to the PSAP is for the purpose of workstation connectivity. This use case does not preclude multiple ESInets from co-existing across the same geographic region; rather it defines a configuration in which a network provider has capacity and resources with which to provide services throughout a region, state, the nation – or even internationally.

Advantages:

- This provides advantages in case of local disaster; the infrastructure serving the PSAP is not necessarily in the affected area.
- Expertise and focus of the provider, which becomes increasingly important as these network solutions become increasingly complex.
- Economy of scale of a shared infrastructure. Given the duplicative services and capacity created as the number of ESInets increases, optimal configurations are achieved through economies of scale serving large geographic regions.
- Originating Service Providers (OSPs) can potentially require fewer points of interface to deliver 9-1-1 traffic.

Challenges:

- Localities may perceive loss of local control by not having facilities near served PSAPs
- May not support historical bias towards having local facilities
- Local jobs may be fewer based on the economies gained through centralized services.
- As the number of tenants increase the Network complexity would increase with a larger number of possible IP routes

The following diagram illustrates the hosted shared ESInet deployment models. The primary concepts of serving many PSAPs, OSP connections and geographic data centers are illustrated.

Hosted Shared ESInet Deployment Models

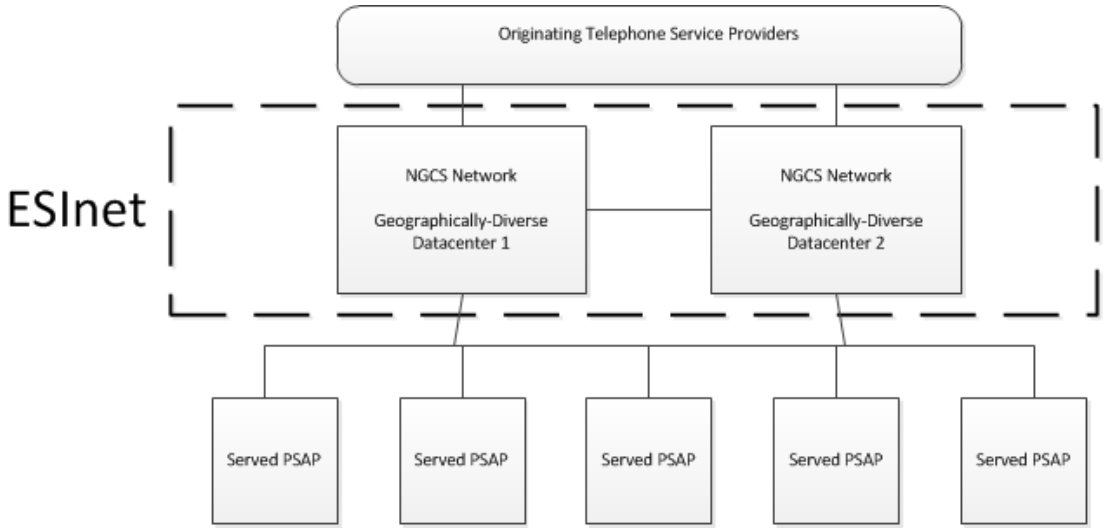


Figure 5-6

5.5.3 Network Monitoring & Operational Metrics

The ESInet should be monitored 24x7 by a Network Operations Center with visibility across the network. Network elements should be alarmed and current network diagrams should

be available to assess any loss of connectivity. This should include a Simple Network Management Protocol (SNMP) system to monitor the devices in the system. Priority should be established for network alarms with service impacts taking top priority. Potential service disruptions such as the loss of redundancy should also be prioritized.

The ESInet is a critical component for end-to-end service delivery, but not the only one as access networks, Next Gen core service providers, local area networks, and customer premise equipment all have a role in successful voice and data delivery. As such, clear rules and responsibilities need to be established and to the extent possible one party have accountability for coordinating across these entities for maintenance and restoral efforts. Operating procedures that include contact information, notification requirements, and escalation points help to address service issues and in some cases avoid a disruption.

Emergency communication networks strive to be reliable with high availability. Five nine's (99.999%) is the goal for availability of these networks and is achieved through various means focused on diversity, redundancy, and alternate routing. While "five nines" is the generally accepted minimum availability service level, it should be noted that this equates to 5.26 minutes of unscheduled downtime or service unavailability per year. Another important factor when comparing network availability to consider is specifically how different network service providers define availability and how it is calculated. For example, scheduled maintenance events are typically not included / classified as downtime. The ESInet by design incorporates multiple paths for voice and data transmission. The failure of a single element within the network or congestion along a path will not necessarily limit the ability to deliver traffic. Availability can be enhanced with multiple ingress and egress circuits, alternate routing to a back-up location, or a parallel network path with transport diversity. The specific approach will need to be developed based on the governing entity's service requirements and funding capability. There can be a variety of approaches that balance circuit diversity, redundancy, and alternative routing to a back-up location and ensure high availability.

When designed appropriately, the IP networks provide alternate paths for voice and data traffic that provide increased reliability and avoid any single point of failure. The bandwidth requirements and delay sensitivity will vary by traffic type. Key performance metrics for an IP based application include Latency, Packet Loss, and Jitter.

> **Latency** is the duration when a packet enters the network to the time it exits the network. It can be measured as a one-way transmission across the network or a round trip. Round-trip latency is measured from a single point and is used most often in the form of a ping that provides insight to the network performance.
>
> **Packet Loss** occurs when one or more packets traveling across the network fail to reach their destination. This typically occurs when network congestion along the path results in packets being dropped. When the offered packets exceed the ability of a particular segment to transmit them, packets are dropped.
>
> **Jitter** occurs when the receipt of packets is out of sequence from what was transmitted. Packets can take more than one route through the network and the delay (latency) across the network can vary depending on the path used. Buffering is typically used to mitigate Jitter and properly sequence packets upon arrival.

All three of these metrics can be indicative of the overall network performance and service quality. Individual provider targets may vary, but packet loss of <1%, latency of <15-20 mS, and jitter variance of <20 mS represent sample targets per NENA document 08-506 "Emergency Services IP Network Design."

5.6 Access and NG9-1-1 Core Services Implementation

Next Generation 9-1-1 implies routing a call based on a caller's location information as provided by the Originating Service Environments (OSE) (a combination of Originating Service Provider, Network Access Provider, Location Information Provider and SmartPhone Apps provider). A 9-1-1 service system in its simplest form is illustrated below:

NG9-1-1 System in Simplest Form

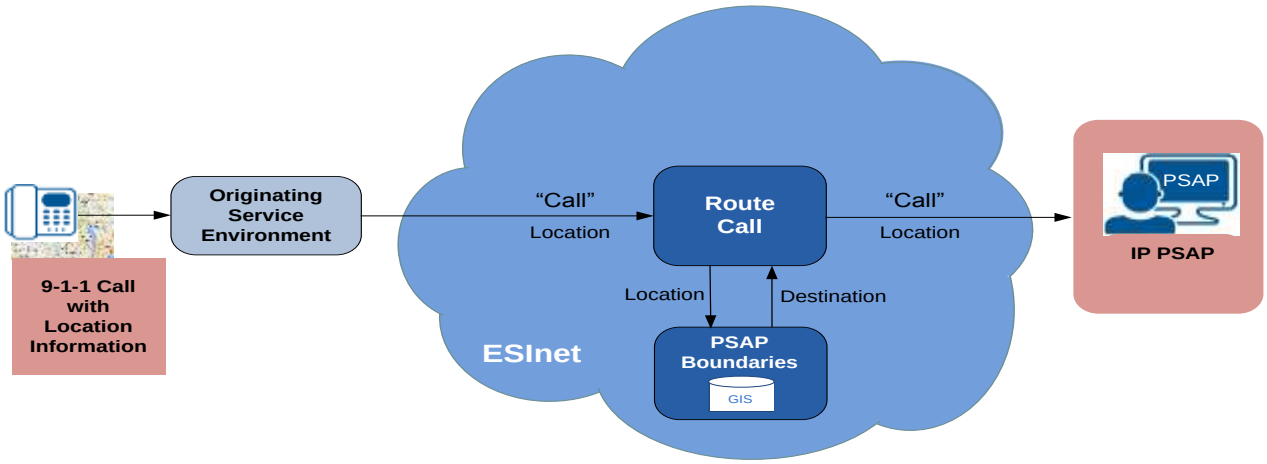


Figure 5-7

Additional complexity is added when it is necessary to determine the responsible Public Safety Authority, as illustrated below (e.g. where the OSP's territory potentially covers multiple PSAPs or Public Safety Authority regions).

Additional Complexity Where OSP's Territory Potentially Covers Multiple PSAPs or Public Safety Authority Regions

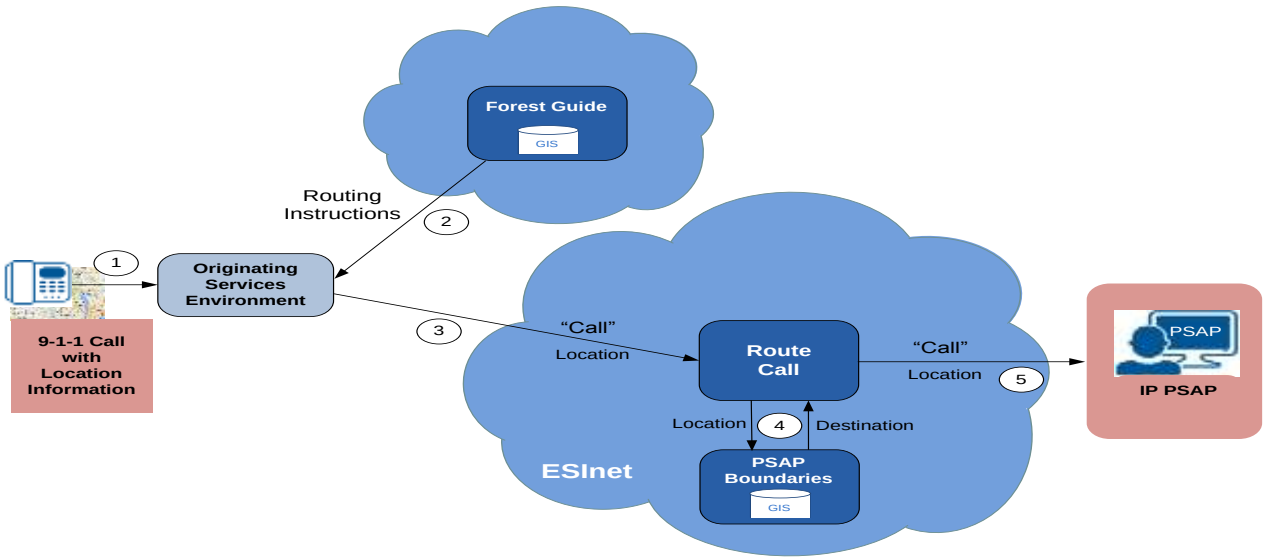


Figure 5-8

5.6.1 Specific NG9-1-1 Access Implementation Options

Next Generation 9-1-1 architecture concepts and functional services do not assume that the Originating Service Environment (OSE) necessarily knows whom the PSAP and/or 9-1-1 Authority is for a given geographic area. In the legacy model the service area of TDM switches was coincident with one (or a few) PSAP(s). In an IP-based world, the user could be in any PSAP and 9-1-1 Authority's jurisdiction. Therefore, NG9-1-1 requires services that make it possible to determine the appropriate 9-1-1 Authority's NG9-1-1 network, in order to then be routed to the appropriate PSAP within that NG9-1-1 system.

Since users can roam with their communication devices across the country or the world, the OSE may potentially need to support connectivity to many Public Safety Authorities.

The OSE has several operations that require interaction with a Public Safety Authority:

- Validate Location Information
- Determine the appropriate Public Safety Authority to receive a 9-1-1 call or message
- Obtain a copy of the rules to validate location information (LVF function)

The OSE must connect to each Public Safety Authority's LVF to determine if addresses they will be providing to the Public Safety Authority's NG9-1-1 system during 9-1-1 call setup are valid addresses according to the given Public Safety Authorities addressing rules.

In order to determine the appropriate Public Safety Authority an NG9-1-1 service (Forest Guide) is provided that allows the OSEs to query and determine the responsible Public Safety Authority or representative of the Public Safety Authority. It is possible, and likely, that an ESInet with NG9-1-1 services represents many Public Safety Authorities. The general Forest Guide concept is a tree structure where an OSE queries at the level for which they know the subscriber/user resides. In some cases, the OSE would query the top level Forest Guide for the United States (National Forest Guide). The Forest Guide returns the "next hop" which may be another Forest Guide function to inspect or the target ESInet with NG9-1-1 services. In general, a Forest Guide is a unique instance of a NENA i3 Emergency Call Routing Function (ECRF) functional entity. The geographic polygons in the NG9-1-1 core services ECRF are simply more granular, pointing to specific PSAPs, then what would be expected in a Forest Guide, pointing to a state service or ESInet with NG9-1-1 services.

GIS Data and Security Services Foundation

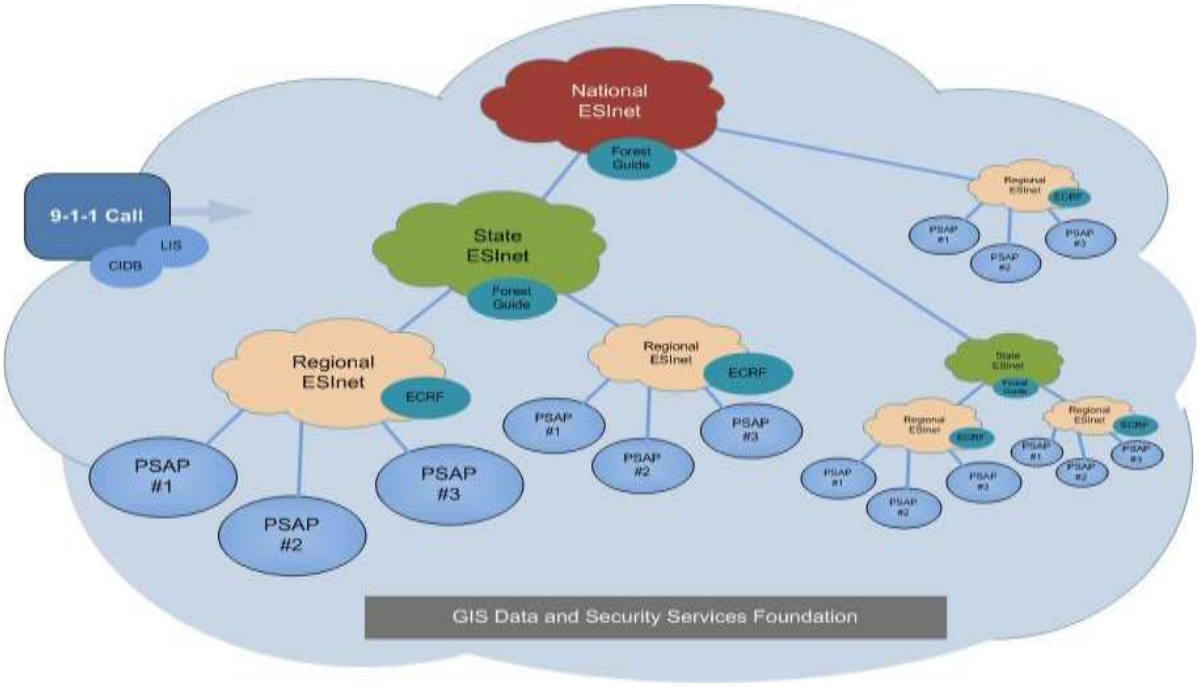


Figure 5-9

The concept of Forest Guides requires cooperative sharing of the respective geographic polygons that define Public Safety Authority's service area. These mechanisms are complex and have many issues to resolve with respect to sharing and change management.

The need to dynamically determine responsible Public Safety Authorities is a NENA i3 end-state architecture requirement. However, during many phases of the NENA i3 transition model the Public Safety Authority is still determined by local infrastructure connectivity and therefore does not require Forest Guides. This is the reason that no NG9-1-1 Forest Guides exist today. The VoIP service providers (VSPs) have a similar issue, but they have long standing network routing control solutions that are used in lieu of the existence of NG9-1-1 Forest Guides.

Inversely to the OSE accessing NG9-1-1 services, conditions exist where the NG9-1-1 Services require access to services provided by the OSE. In the full concept of NG9-1-1, OSEs would have Location Information Servers (LIS) and Customer Information Data Bases (CIDBs) that would provide this data upon query from various NG9-1-1 systems. In the transitional period, location data is acquired from the ALI servers, (typically provided by third party vendors), etc. that are `standing in' for the LIS and the CIDB functions. Existing ALI servers are being retrofitted to accept NG9-1-1 protocols and provide the functions of the LIS and the CIDB during an unknown transition period.[49] Various forms of access needs in these areas will continue for the foreseeable future.

If third party vendors continue to evolve services to support the above, then consolidation of these processes may mean that multiple NG9-1-1 systems connect to these

[49] See NENA-INF-008.2-2014, NG9-1-1 Transition Planning Guide Considerations Information Document

vendors, rather than there being access connections for each NG9-1-1 system separately. While and where stand-alone ESInets exist, multiple OSPs would need to access multiple ESInet points. With the proper ESInet interconnectivity in or among regions and states, these access connections could become simplified. Analogous options exist for call and messaging access to multiple NG9-1-1 systems, utilizing the `Forest Guide' structure.

NG9-1-1 involves periodic and continuous evolution for the foreseeable future, both in access methods and in the NG9-1-1 core services interfaces.

5.6.2 National Forest Guide

Fundamentally required if the NENA i3 end-state operational model is realized.

Advantages

- Ubiquitous solution for determining 9-1-1 call management responsibilities

Challenges

- Fundamentally required if the NENA i3 end-state operational model is to be realized.
- A nationwide access implies significant security challenges
- Complex data distribution and change management model
- Who will fund the National Forest Guide
- Who will operate the National Forest Guide (whether outsourced responsibility or not)
- Will all ECRF Guides representing states or entities below the National Forest Guide exist and operate appropriately
- Will the foundation GIS data for Forest Guides be properly managed and distributed as necessary

5.6.2.1 Service Utilizing Forest Guides

One of the fundamental problems in routing of emergency calls is to determine which Public Safety Answering Point (PSAP) to direct the call to. In the general emergency services architecture originally developed by the Internet Engineering Task Force (IETF), mapping between the caller's location and the destination PSAP is obtained using the Location-to-Service Translation Protocol (LoST) defined in Request For Comment (RFC) 5222.[50]

Since each Emergency Call Routing Function (ECRF) or Forest Guide only contains service information relating to a specific geographic area, in order to route an emergency call, it is necessary to locate the ECRF with the mapping information specific to the caller's location. These are referred to as authoritative servers because the data has been compiled and loaded by the entity responsible for ensuring the correctness of this data.

Forest Guides enable geographically and logically dispersed the ECRFs to operate as a coherent whole somewhat resembling the hierarchical model used by the Domain Name Service (DNS), with the hierarchy based on geographical and service boundaries.

In practice Forest Guide architectures may be operated at the National, State or Regional levels. Also, Forest Guides may be reachable over the public Internet, or queries may only be

[50] https://tools.ietf.org/html/rfc5222

accepted from within the ESInet. Finally, call routing and emergency call termination may be provided for arbitrary applications, or only for applications with termination agreements. The sections that follow examine the implications of these choices.

5.6.2.2 Mapping: Internet vs. ESInet Access

The original IETF architecture assumed that a calling device making an emergency call would obtain its location and then query a LoST server to determine where to direct the emergency call. This required the LoST servers to be reachable over the Internet by any device/application capable of making an emergency call. The ECRF and Forest Guide solution included within NENA i3 is based on the IETF approach model in which the LoST servers are accessible on the public Internet.

Allowing the LoST servers to be accessible via the Internet provides maximum flexibility for applications making emergency calls. However, it also enables adversaries to attack the 9-1-1 emergency service system from the Internet.

By only allowing ECRF queries to be handled from within the ESInet, attacks on the emergency service system can be limited to attackers with access to the emergency network. Rather than requiring mapping data to be published to publicly facing entities, if the mapping service is only accessible from within the emergency network, only trusted entities are ever queried and only authorized entities are permitted to query the Forest Guide. Accessing entities are expected to be validated and authorized. This is further discussed below.

The level of vulnerability of the NG9-1-1 system to attackers within an emergency network depends on the level of connectivity between emergency networks. In order to allow the network of Forest Guides to function when location-mapping queries are only enabled from within the ESInet, ESInet connectivity needs to be provided commensurate with the level of administration. For example, a National Forest Guide accessible from the ESInet requires connectivity between ESInets nation-wide; State Forest Guides require connectivity within statewide ESInets, etc.

5.6.2.3 Application Restrictions

The rapid adoption of smartphones and the increasing popularity of mobile emergency service applications is one of the major areas of technological innovation within NG9-1-1 today. With applications catering to the needs of a wide range of demographic groups including families, college students/universities, retirees, the disabled, etc. mobile emergency service applications have the potential to have a major impact on the evolution of NG9-1-1.

Rather than allowing emergency calls to be placed from arbitrary applications, calls connecting to the ESInet typically require interconnection agreements to be in place, with the service provider directing calls to the ESInet being accountable to some extent for the authenticity and the validity of information provided with the call. In order to enable deployment of emergency mobile applications, applications providers could be allowed to act as “service providers”. While this imposes a hurdle on the development of new emergency services applications, it also offers a way to limit damage from rogue applications. The balance between the ease of access and mitigation of attack or destructive impacts becomes a matter of policy and cybersecurity.

5.6.2.4 Forest Guides Governance and Funding

5.6.2.4.1 Governance and Funding Issues

The establishment and operation of a National Forest Guide is likely to require development of funding and governance models as well as interoperability requirements and operational procedures. These requirements and procedures would in turn dictate the information to be pushed from lower-levels to higher-levels, and the frequency with which the data replication would occur.

Solutions that minimize the complexity and volume of data exchanges also minimize upstream dependency on this data and so minimize the need for imposition of national requirements and procedures at the state and local level.

5.6.2.4.2 NENA National Forest Guide Management

In Figure 6-4, geographic mapping information is populated and maintained within local or regional LoST servers (ECRF databases). The data is then published to nodes deemed to be "higher up the tree". These higher-up nodes are then responsible for combining and compiling all of the data form the leaf-nodes so that they can provide a consistent view to their higher-up nodes and so on. The identity of the authoritative server is always maintained with the data so that it is easy to determine from where it originated. All of this leads to a significant amount of data transfer and processing, and small changes at the county-level may result in republication of state information to a National Forest Guide.

National Forest Guide Hierarchical Data Roll Up

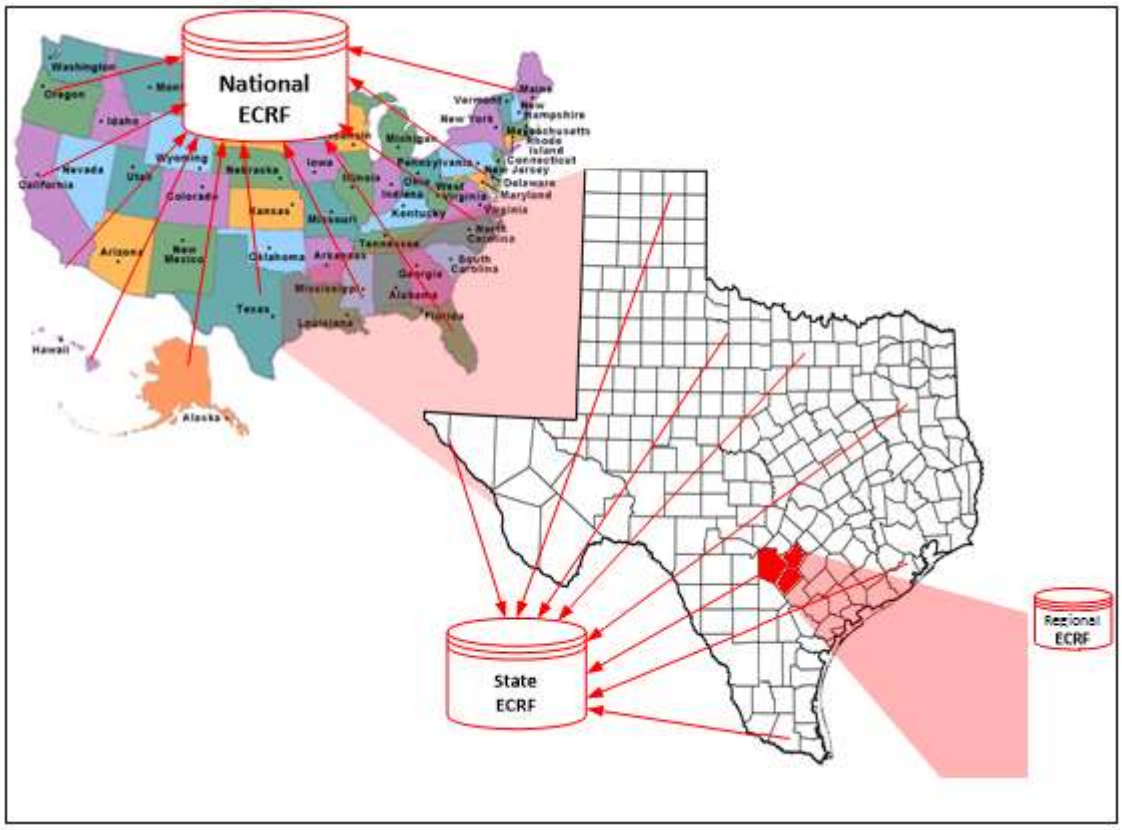


Figure 5-10 (Texas is used for illustrative purposes only)

Advantages:

- Significantly simplifies routing discovery function; all discovery can be accomplished through the National Forest Guide.
- Provides a national approach so that any device/entity can determine the correct route for an emergency call, providing the data is populated into the ECRFs. Employs international standards.

Challenges:

- Requires consistent operating procedures across all levels and regions.
- Requires massive volumes of data to be acquired and groomed if all boundary information is at the National Forest Guide level.
- Requires massive volumes of data to be transferred between entities if all boundary information is at the National Forest Guide level.
- Requires funding model for the National Forest Guide. All devices/entities must support both redirection (if the LoST service is publicly reachable) and recursion.
- Significantly increases load at the national Forest Guide level if all queries go through the national Forest Guide.

5.6.3 Statewide

In the figure below, geographic mapping information is populated and maintained within local or regional ECRF servers.

State Forest Guide Hierarchical Roll Up

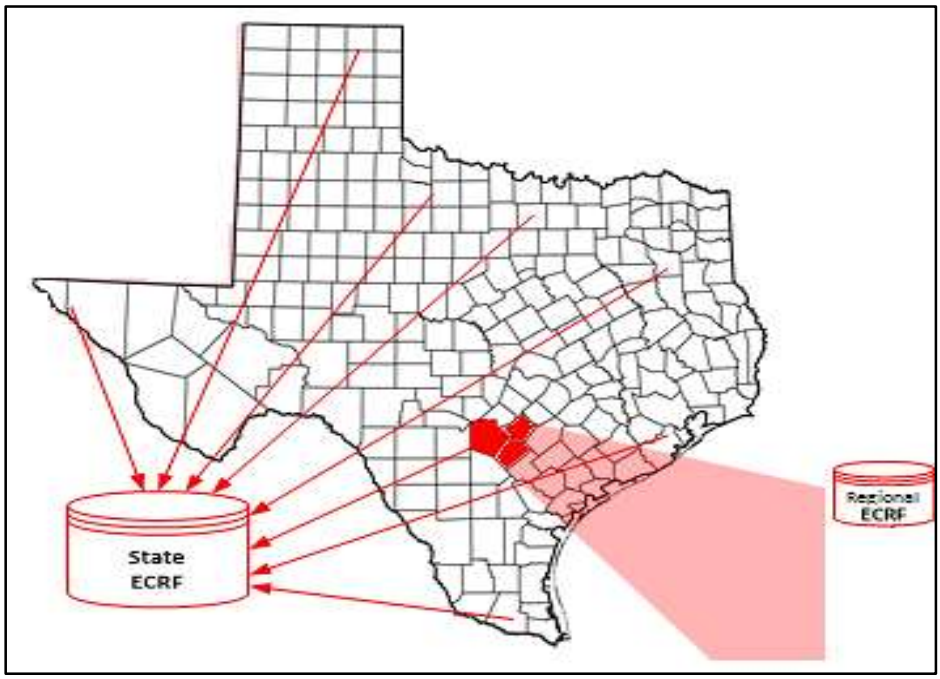


Figure 5-11 (Texas is used for illustrative purposes only)

The data is then published to the statewide nodes, which provide a consistent view within the state. The identity of the authoritative server is always maintained with the data so that it is easy to determine from where it originated. Data transfer occurs only within the state so that changes at the county-level do not propagate beyond the state.

However, in the absence of a National Forest Guide, it is no longer possible to query any ECRF server and receive in response a Universal Resource Identifier (URI) pointing to the destination state ECRF or regional ECRFs within the state. Instead, individual statewide ECRF servers need to be queried – and if the location is outside the state, this could imply querying multiple statewide ECRF servers in order to obtain a response.

If the statewide ECRF servers are reachable over the Internet, then emergency services applications would need to be configured with the names of the statewide ECRF servers. If statewide ECRF servers were not reachable over the Internet, then either a National Gateway would need to be provided that could query the state-level ECRF servers in order to route calls, or individual State Gateways would need to be provided, serving as entry points to the emergency network within each state. If the State Gateways do not emerge or were not configured in a consistent manner, then the result would be additional complexity exposed to originating service providers.

Advantages:

- Reduces the volume of data that needs to be transferred as compared to maintenance of data for a national Forest Guide
  - Transfers only occur between the local and state levels.
- Funding model for State Forest Guide can be determined within each state.
- Employs international standards.

Challenges:

- Complicates the routing function since queries must now be directed to the correct State Forest Guide in order to receive a successful response. (This is workable since there is a high probability that the OSP would know the state in which their customer is located, and therefore which state to query.)

5.6.4 Regional

If Access is regional, corresponding to a regional NG9-1-1 service system, then the NG9-1-1 Core Services provides the routing function, through the ECRF and ESRP process, to the related PSAPs. However, if the NG9-1-1 systems are implemented at lower than regional level, then there may need to be a regional level routing process to differentiate between the subtending NG9-1-1 systems based on originating caller location.

Advantages:

- Creating a Regional Access model provides a template for local ECRF server authorities to include in their initial architecture build.
- Provides a forum for Local entities to communicate with neighboring authorities to build in the proper URI ‘pointer response’ to a non-local query.
- Ensures 9-1-1 calls destined for termination points within the Region are routed correctly

Challenges:

- Requires leadership, cooperation and funding,
- Ongoing administrative process and procedures may require interoperable arrangements

5.6.5 Local Access

If NG9-1-1 Core Services were implemented at a local geographic level (such as an individual County), then they would be accessed either locally or at higher levels via regional or state gateways and since NG9-1-1 would not initially be interconnected to other local areas as is the case when implemented regionally or at statewide levels.

Advantages:

- Inter-governmental relationships are minimized
- Initial local implementations can be transitional toward a later more collaborative approach in a host or hybrid configuration.

Challenges:

- If not interconnected with neighboring systems, then routing outside of local boundaries requires additional technical solutions and adds complications
- May require substantial work to redesign the local ECRF functionality in the event a Regional model is deployed at a later date
- Complicates potential communication and collaboration between local NG9-1-1 deployments by creating a barrier to interoperability

In all cases above, it is assumed that customer data provision and validation processes would be implemented at the related level of NG9-1-1 system implementation, unless a third party provided an aggregation service between multiple service providers and multiple 9-1-1 system service providers.

5.6.6 Specific NG9-1-1 Core Services Implementation Options

The TFOPA has studied NG9-1-1 implementations that are being accomplished around the nation. It is clear that certain operational functions provided by PSAPs must remain at the local level. However, there are architectural functions of NG9-1-1 core services that should be done at a regional, statewide or national level. The PSAPs must continue to provide operational aspects of 9-1-1, emergency communications and dispatch functionality. However, operations of the Core Service elements of NG9-1-1 most effectively and economically occur above the local level. This approach must include regional and state level collaboration for cost effective implementation and the ability to provide backup capabilities.

5.6.6.1 9-1-1 Services Architecture

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 more complete NG9-1-1. Next Generation 9-1-1 systems implies changes not only to the 9-1-1 System Service Provider and PSAP operations, but also at Originating Service Providers (OSPs)

who provide communication services to subscribers and deliver 9-1-1 calls through the central NG9-1-1 Core Service system. Access Network Providers who provide Location Information service are also impacted.[51]

The 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
- NENA i3 Vision Long Term NG9-1-1 Architecture (NENA Standard STA-010.2)

The legacy architecture is very common and more or less consistent across the United States. The transitional architectures are intermediate steps that replace the legacy architecture with an IP technology foundation. The NENA i3 NG9-1-1 architecture requires fundamental changes in roles and responsibilities, the underlying data and the steps to process calls. Fundamentally, the way the Originating Service Environment (OSE) prepares data and delivery calls to Regional 9-1-1 Systems Service Providers changes from legacy approaches to NG9-1-1. Each of the 9-1-1 architectures has two basic areas:

1. Pre–call data preparation
2. Steps performed to process a 9-1-1 Call, including use of core services features during and after call delivery

The pre-call data preparation creates a necessary foundation for each call time processing scenario. The legacy architecture prepared predetermined static data relationships that were required to exist prior to successfully routing a 9-1-1 call. The NG9-1-1 architecture determines call routing dynamically based on the caller's location and jurisdictional service boundaries.

5.6.6.2 Legacy 9-1-1

The foundation of the Legacy 9-1-1 architecture is the creation of a set of rules used to validate subscriber addresses. The Master Street Address Guide (MSAG) contains a set of rules that determine whether an address is acceptable to the 9-1-1 Service Provider. If an address is recognized and passes MSAG validation, then it is determined that the address is "dispatch-able", meaning that an emergency services first responder should recognize the address unambiguously. These dispatch-able addresses help determine the exact location to send emergency services.

In addition to validating addresses, the MSAG creates a relationship between addresses and Emergency Services Numbers (ESNs). Addresses or address ranges are assigned an ESN. An address range is a specific locality's street name and an address range such as "all the even addresses on Main Street 1002 through 2000". Therefore, an address of "1226 Main Street" would pass validation for the given locality. The ESN designates the primary and alternate destinations that should receive the 9-1-1 call for the corresponding set of TNs assigned with that ESN. The ESN destination is usually a PSAP, but also could be a Public Switched

[51] NENA 08-003 Page 16, Access Network Providers (e.g., DSL providers, fiber network providers, WiMax providers, Long Term Evolution (LTE) wireless carriers, etc.) have installed, provisioned and operated some kind of location function for their networks. Location functions are critical for 9-1-1 calls originating on an IP network because it provides a 9-1-1 valid location to IP clients that bundle their location in the SIP signaling to the ESInet. Last Accessed December 2, 2015 http://c.ymcdn.com/sites/www.nena.org/resource/resmgr/Standards/08

Telephone Network (PSTN) phone number. The ESN also may designate the emergency service providers (e.g., Police, Fire, Medical) for the specific area if the given Regional 9-1-1 Service Provider utilizes Selective Transfer features.

The legacy 9-1-1 architecture is based on the OSPs providing content from their Subscriber Service Order (SO) records to each Regional 9-1-1 Service Provider. The OSP subscriber records include the Subscriber's address, class of service and telephone number. These SO based records are the MSAG validated and assigned an ESN. After this process is completed, the addresses are posted in the Automatic Location Identification (ALI) database and the TN ESN relationship is posted in the Selective Routing Database (SRDB).

A legacy 9-1-1 call progresses from the OSP to the legacy selective router (SR) over TDM trunks, typically Signaling System 7 (SS7) protocols. The legacy SR determines the PSAP to receive the call, typically using the telephone number of the subscriber (Automatic Number Identification or 'calling number') to retrieve an ESN from the SRDB. The SR then directs the call to the PSAP and that has typically been over legacy TDM trunks called CAMA trunks, again passing ANI to the PSAP. The PSAP receives this call and uses the ANI to retrieve location information from the ALI database and displays the location and call information to a 9-1-1 call taker. This is a simplistic scenario that does not address all of the variations that can occur, but does represent a basic call flow. (The TDM trunks to the PSAPs have often been replaced with digital or even IP connectivity to reduce costs and provide faster call delivery to the PSAP.)

Wireline calls are the most straightforward legacy call processing scenario, since the legacy 9-1-1 solution was designed for fixed location or the Wireline telephone service model. Wireless, VoIP and Text Messaging all have workarounds due to the limitations of the legacy 9-1-1 operating environment. These workarounds, not described here, have allowed the legacy architecture to adequately address the processing of wireless and VoIP 9-1-1 calls. However, the legacy-operating environment has become more complicated with these workarounds and is not extensible to support new features or new forms of "calls for help". As a result, NENA began design of a new 9-1-1 service system in 2001, now known as NG9-1-1.

5.6.7 NENA i3 Vision

The NENA i3 vision Long Term architecture standard changes the processing model for 9-1-1 calls and defines different responsibilities for both the 9-1-1 Service Provider and OSEs. The biggest changes evolve around the use of Geographical Information System (GIS) technology and OSEs providing the caller's location information during call setup.

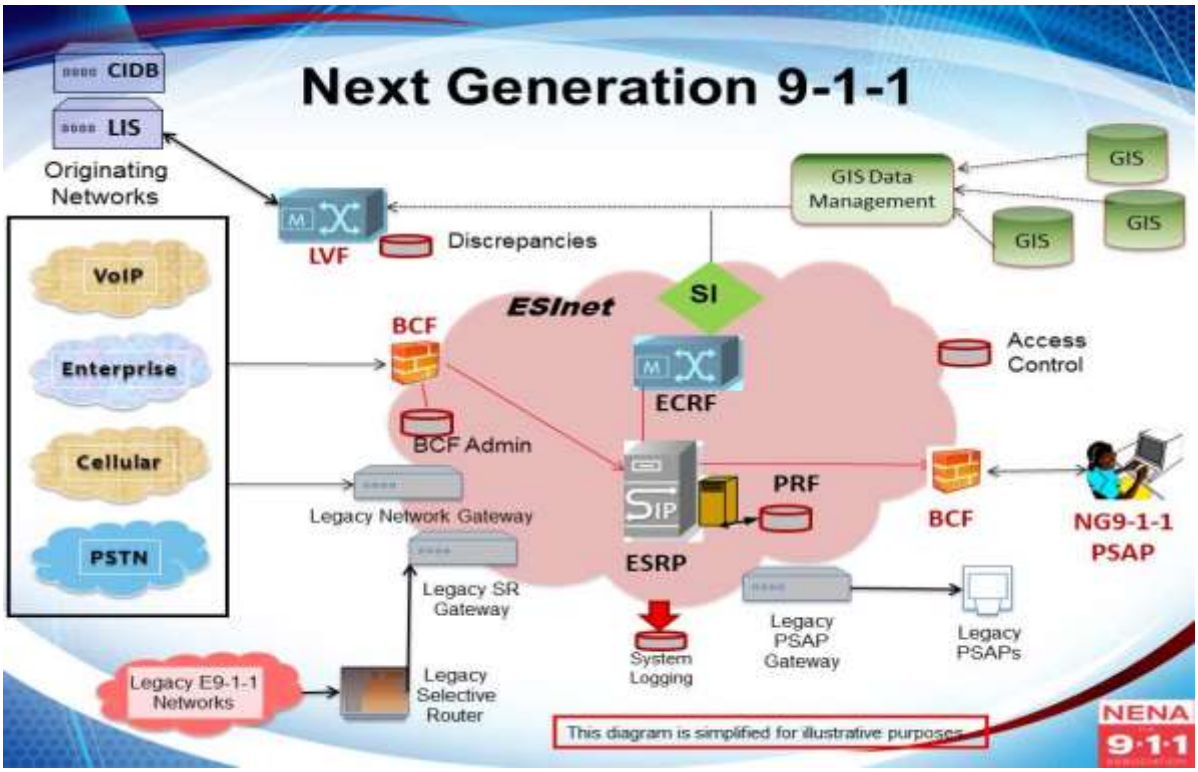


Figure 5-12

The local 9-1-1 Authority shifts from managing the MSAG for address validation purposes to managing basically the same data, minus the ESN, in a GIS tool. The GIS tool incorporates the address validation data of the MSAG and also includes jurisdictional boundaries of PSAPs and optional boundaries of emergency service providers. The legacy ESN is dropped and replaced with an algorithm at call processing time that locates the caller's location within the set of jurisdictional polygon boundaries. The elimination of the ESN with this dynamic "location within a service boundary" algorithm greatly simplifies 9-1-1 data management and the number of changes necessary to implement routing changes. Also, the 9-1-1 Service Provider is expected to provide an address validation service; the Location Validation Function (LVF), is used by the OSE for 9-1-1 data preparation.

The OSE responsibilities are also changed. The OSEs are no longer expected to deliver their SO record content to the 9-1-1 Service Providers. Instead, OSEs retain their subscriber and address information in a Location Information Server (LIS). The OSEs access LVFs provided by 9-1-1 Service Providers to ensure their location information is acceptable for 9-1-1 purposes. The OSEs deliver their calls via IP technology and retire Time Division Multiplexing (TDM) circuits. The OSE delivers caller location, or the ability to retrieve caller location information, co-incident with the 9-1-1 call to the 9-1-1 Service Provider. The OSE has the option of delivering the location with the call signaling messages or providing a reference key so the receiver of the call can retrieve the caller's location later. The 9-1-1 callers that are calling from a device that allows mobility are the primary example of when an OSE should provide a location reference for retrieving the caller's location.

The transition to IP technology requires various security and networking appliances to be introduced to the 9-1-1 Service Provider domain. Border Control Functions (BCFs), including Session border controllers, firewalls, intrusion detection, and identity verification solutions all

must be incorporated into the NG9-1-1 solution. Various cybersecurity policies and procedures, as described elsewhere in this report, apply at physical network, NG9-1-1 software, and database levels. The NENA i3 architecture standard also includes the ICAM (Identity, Credential and Access Management) procedures to control user access based on their roles in operations or maintenance activities. While it is recognized that the ICAM in the larger sense has multi-system involvement, the NENA standard does not speak to details of integrating the ICAM with other related systems in the Public Safety environment. It does include various functions and features not discussed here that provide routing control and post-call delivery functionality not previously available in the E9-1-1 environment.

An i3 architecture call begins with the OSE accessing the caller's location information and signaling the 9-1-1 System Service Provider that a 9-1-1 call is available. These messages will pass through the NG9-1-1 system Border Control Functions. The NG9-1-1 core services system obtains the caller's location information and, combined with jurisdictional boundaries from a GIS database, determines the serving PSAP. Any special conditions the PSAP may have set are checked in the Policy Routing Function (PRF) and the call is delivered to the designated PSAP. If the call was delivered with a "Location by Reference" approach, then the PSAP can use the reference information to retrieve updates of the caller's location information.

In addition to the elements described above, additional functions are required when an all IP call-processing environment is established. Specifically, a function called the "Forest Guide" will allow an OSE to determine which NG9-1-1 Service system (via ESInet) to send a given 9-1-1 call.

5.6.8 Evolutionary NG9-1-1 Architectures

Several aspects of the NENA i3 long-term vision architecture are barriers to immediate implementation. Primarily, OSEs 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 evolutionary architectures exist.

- IP Selective Router (IPSR) – essentially E9-1-1 on an IP network
- NENA i3 Transitional Architecture

An IPSR transition architecture replaces the legacy SR with the IP infrastructure and continues to process 9-1-1 calls based on the callers ANI and a mapped ESN. Essentially this is E9-1-1 utilizing an ESInet as the IP transport. 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.

The NENA i3 transitional architecture introduces elements to map legacy interfaces to NENA i3 architecture defined interfaces and provide the caller's location information during call setup. Calls from OSPs can be delivered via legacy TDM circuits into gateway devices that convert TDM protocols to IP protocols. These gateways, or Legacy Network Gateway (LNGs), provide protocol conversion functions and are the defined functional element to retrieve the caller's location information and send it through the other i3 processing elements to complete call processing. Note that the NENA i3 document defines these elements as "logical" and not necessarily "physical" real world devices. A NENA i3 logical functional element may be satisfied by one or more physical processing elements.

An additional gateway element is defined for interacting with legacy SRs, the Legacy Selective Router Gateway (LSRG), and an element is defined for interacting with legacy PSAP call handling equipment, the Legacy PSAP Gateway (LPG). These elements all provide protocol conversion and allow the NENA i3 functions to interact with legacy 9-1-1 equipment and interfaces. Note that this approach allows legacy PSAPs only limited utilization of the NG9-1-1 core services features.

Call processing is accomplished as defined by the NENA i3 architecture with the exception that the gateways provide protocol conversion and the caller's location information is retrieved from some source that is not necessarily the OSE. In practice today, the caller's location is often being retrieved from or through the legacy ALI database.

5.6.9 NG9-1-1 Implementation Options

5.6.9.1 Multi-State Hosted

This model uses a geographically distributed set of redundant NG9-1-1 functions and an associated ESInet to support areas of the NG9-1-1 service and related PSAPs within and across multiple states. The architecture supports a multi-tenant model where many PSAPs or 9-1-1 jurisdictions have a perception of a dedicated set of NG9-1-1 services even though the infrastructure is supporting various unassociated PSAPs. Regional facilities are deployed as necessary, such as Legacy Network Gateways to collect the TDM call traffic. Those regional facilities are connected back to two or more core processing centers that contain the majority of the NG9-1-1 Service functions (e.g., ESRP, ECRF, BCF, DNS, and Logging Service).

The architecture serving the PSAPs would not have more than one Core site near the served PSAPs and actually may not need any core sites physically near the served PSAPs. Today's IP broadband networks make the physical location of core sites nonmaterial; therefore the benefits of distributing core NG9-1-1 functions can be realized. The trend toward OSPs moving away from TDM circuits and connecting via IP also benefits this model. Efficiencies and benefits of scale are created by OSPs connecting to a few geographically distributed NG9-1-1 services core sites.

The Multi-Stated Hosted model has the following advantages and challenges.

Advantages:

- In case of local disaster, the infrastructure serving the PSAP(s) is not necessarily in the affected area.
- Enables development of specific expertise and focus of a provider, which becomes increasingly important as these solutions become increasingly complex.
- Economy of scale of a shared infrastructure. Given the duplicative services and capacity created as the number of NG9-1-1 systems increases, optimal configurations are achieved through economies of scale serving large geographic regions.
- Troubleshooting and recovery may be enabled by larger service system size and impacts under one management structure.
- Originating Service Providers (OSPs) can connect to fewer points of interface to deliver 9-1-1 traffic.

Challenges:

- Localities, regional and state level 9-1-1 Authorities may perceive loss of control by not having 9-1-1 systems near served PSAPs or within related regulatory and legislative boundaries.
- Disrupts historical tendency towards having central 9-1-1 services in vicinity of jurisdictions.
- Local jobs may be fewer based on the economies gained through centralized services.
- As the number of users increase, the 9-1-1 service system complexity would increase with a larger number of possible IP routes
- Troubleshooting and recovery along with service area impacts may be may be more complicated and larger.

5.6.9.2 Statewide

In this scenario, the NG9-1-1 Core Services is implemented for statewide use by all 9-1-1 Authorities, under a state-level organized governance structure, which should also include regional or local government representatives for planning and management decision making. NG9-1-1 may be operated on a single statewide ESInet or multiple interconnected ESInets, which may support other Emergency Services applications at state or more localized levels.

The architecture supports a multi-tenant model where many PSAPs or 9-1-1 jurisdictions utilize a dedicated set of the NG9-1-1 services. Two or more locations for access points, either individually and/or via a state level Forest Guide, are deployed as necessary. Access facilities are connected to two or more duplicated, geographically diverse core processing centers that contain the majority of the NG9-1-1 Service functions (e.g., ESRP, ECRF, BCF, DNS, and Logging Service).

Advantages

- NG9-1-1 core services and management/administration costs are spread across many 9-1-1 Authorities for a single NG9-1-1 core service system – lessens impact on local funding compared to other choices
- Common procedures for the above are established
- Makes access structure for the OSPs simpler than lower level implementation choices
- More directly supports interoperability due to common architecture and procedures
- Makes shared and hosted facilities and equipment more workable
- Involves planned multi-level governance arrangements
- May make cybersecurity and physical security simpler than other choices

Challenges

- Survivability is potentially affected by limited geo-diversity of service, beyond the normal duplication and diversity of data centers supporting NG9-1-1 core services
- Requires planned multi-level governance arrangements
- Involves potential political issues and changes
- Probably requires new legal arrangements, such as governance and funding aspects
- Requires specific plans for and implementation of inter-state ESInet connectivity to support interoperability

5.6.9.3 Regional

In this scenario, NG9-1-1 Core Services is implemented for multi-county or multi-PSAP use by all associated 9-1-1 Authorities, under a sub-state level organized governance structure, which should also include local government representatives for planning and management decision making. Next Generation 9-1-1 may be operated on a single statewide or region-wide ESInet or multiple interconnected ESInets within the region, which may support other Emergency Services applications at state or more localized levels.

The architecture supports a multi-tenant model where many PSAPs or 9-1-1 jurisdictions utilize a dedicated set of NG9-1-1 services. Two or more locations for access points are deployed as necessary, such as Legacy Network Gateways to collect TDM call traffic. A state-level Forest Guide may support access. Access facilities are connected to two duplicated, geographically diverse core processing centers that contain the majority of the NG9-1-1 Service functions (e.g., ESRP, ECRF, BCF, DNS, and Logging Service).

Advantages

- NG9-1-1 core services and management/administration costs are spread across multiple 9-1-1 Authorities for a single NG9-1-1 core service system – less impact on local funding compared to more localized choices
- Common procedures for the above are established
- Makes access structure for OSPs simpler than local implementation choices
- More directly supports interoperability due to common architecture and procedures
- Makes shared and hosted facilities and equipment more workable
- Involves planned multi-level governance arrangements
- May make cybersecurity and physical security simpler than more localized choices

Challenges

- Survivability and reliability is potentially affected by limited geo-diversity of service, beyond the normal duplication and diversity of data centers supporting NG9-1-1 core services
- Requires planned multi-level governance arrangements
- Involves potential political issues and changes
- Probably requires new legal arrangements re governance and funding aspects
- Requires specific plans for and implementation of inter-regional and inter-state ESInet connectivity to support interoperability

5.6.9.4 Localized Scenario

Next Generation 9-1-1 Core Services is implemented for a single county PSAP or set of PSAPs, under a locally organized governance structure, which should include local government representatives for planning and management decision making. Next Generation 9-1-1 may be operated on a local or shared ESInet, which may support other Emergency Services applications at state or more localized levels.

The architecture supports a multi-tenant model where several PSAPs or 9-1-1 jurisdictions utilize a dedicated set of NG9-1-1 services. Two or more locations for access points are deployed as necessary, such as Legacy Network Gateways to collect TDM call traffic. A state-level or regional Forest Guide may support access. Access facilities are connected to two duplicated, geographically diverse core processing centers that contain the majority of the

NG9-1-1 Service functions (e.g., ESRP, ECRF, BCF, DNS, and Logging Service).

Advantages

- Requires only local procedures

Challenges

- Survivability and reliability is potentially affected by limited geo-diversity of service, beyond the normal duplication and diversity of data centers supporting the NG9-1-1 core services
- Usually not economical compared to other choices, unless the intent is to have a local NG9-1-1 implementation expand to a regional approach after initial deployment in a single County, and utilize cost sharing across all resulting counties (or equivalent). Higher impact on local funding compared to other choices
- Makes access structure for the OSPs more complex than other choices
- Interoperability beyond the local system is more difficult
- May make cybersecurity and physical security more costly and more difficult to implement and sustain than other choices

5.7 Governance

5.7.1 General Governance Considerations

The Miriam Webster dictionary defines governance as:

- To officially control and lead (a group of people): to make decisions about laws, taxes, social programs, etc., for (a country, state, etc.)
- To control the way that (something) is done
- To control or guide the actions of (someone or something).[52]

The governance of PSAPs and 9-1-1 systems may include any and all of these concepts.

The PSAP governance challenges are complicated. While technological issues related to resource sharing can be challenging, governance may present even more complex, less straightforward issues. Resource sharing and consolidation could be defined to include the sharing of contracts, virtual infrastructure, brick and mortar infrastructure, staff, or all of the above. However it is defined, decisions regarding governance are extremely important. As stated by Mr. Barry Furey in comments made at the 2015 annual conference of the Association of Public Safety Communications Officials, "Consolidation can work in many forms, under a variety of management and funding scenarios. This leads us to the key issue in consolidation - politics. The technical issues can typically be effectively solved. The real work involves getting the buy in required to both take the leap and to maintain the continued support required to continue operation... Yes, a technology roadmap is required, but the most pressing issue is the creation of governing memoranda of understanding and/or interagency agreements."

5.7.1.1 Moving from an Independent to Interconnected System

It is important to understand how the original, or legacy, 9-1-1 system was established. The first 9-1-1 systems in this country were like the first law enforcement agencies in this

[52] Miriam Webster Dictionary, webster.com/dictionary/govern" http://www.merriam-webster.com/dictionary/govern, last accessed October 12, 2015

country. Each was responsible for a specific area or region and operated independent of each other. The advent of NG9-1-1 will change the 9-1-1 governance model and basic elements of the 9-1-1 "culture." In the legacy 9-1-1 environments, it was not technically possible for PSAPs to be fully interconnected, and therefore each PSAP tended to function as an independent agency. With each PSAP operating independently, governance was naturally decentralized, and governance models varied greatly, in terms of authority, responsibility, and the location of 9-1-1 agencies within local and state governments.

This decentralized model has been in place for over 40 years, and despite significant variances, it has generally worked well in meeting the primary objective of providing 9-1-1 service to citizens. The PSAPs increasingly work together each day, with multiple goals including enhancing their operational effectiveness by utilizing various partnership models. Many states now authorize regional or statewide "9-1-1 Authorities" by statute that provide financial and 9-1-1 service support to their member jurisdictions – a concept even more important for NG9-1-1. But, even where such statutory environment does not exist, there are multiple instances of PSAPs working together on NG9-1-1 implementation. For example:

- **The Counties of Southern Illinois Next Generation 9-1-1 Project**. Stakeholders in this project are 17 emergency telephone system Boards in southern Illinois, who have bound together through inter-governmental agreements to create a secure public safety broadband network. Their intent is to, "share voice and data associated with a next generation capable 9-1-1 system," and, "provide future services at a substantial savings to each agency by sharing costs and technology."[53]
- **Pennsylvania Emergency Management Agency**. Pennsylvania is implementing NG9-1-1 via the deployment of multiple regional ESInets. One of the projects is designed to develop a thirteen county ESInet in South Western Pennsylvania, which allows for cost savings through the sharing of equipment and networks, and is planned to be the foundation for the NG9-1-1 core services implementation in that area of the state. This deployment is designed to help ensure that implementation of NG9-1-1 capability across the Commonwealth is completed in the most cost efficient, timely, equitable, and reliable manner possible.

Next Generation 9-1-1 increases the opportunity for PSAPs to share resources and to cooperate and collaborate at multiple levels with potentially greater economic and technical efficiencies. Next Generation 9-1-1 technology has the potential to assist local stakeholders in their pursuit of shared models like "regionalization thru technology," (e.g., hosted, cloud, hybrid) and to lead to a consolidated approach. The PSAPs could begin to identify common challenges that have been listed throughout this document like regional mapping, hosted CPE, CAD, shared voice logging, shared telephony, etc., and through discussion and careful planning, explore how they can best coordinate activities and share resources. Next Generation 9-1-1 moves us away from the legacy system to a place where "sharing" and "synergy" become the norm among local, regional or state connected PSAPs. Sharing resources brings challenges and opportunities to technical aspects such as cybersecurity, as well as nontechnical issues like consistency, uniformity, cooperation and collaboration. While these concepts will be discussed in greater detail in the following sections, further research is warranted to document if these efficiencies exist, to what extent and how different implementations can optimize these

[53] Counties of Southern Illinois Next Generation 9-1-1 Project. http://jc9-1-1.org/index.php/nextgen-9-1-1-project last accessed December 2, 2015

efficiencies.

A common plan for NG9-1-1 implementation facilitates discussion and begins to identify common public safety benefits. A common plan facilitates developing a more regional governance approach that could lead to resource sharing. The PSAP stakeholders may realize that NG9-1-1 allows for more centralized operations and provides for more flexible management options. Many of the more intrinsic problems faced by the current legacy consolidation model may be addressed and resolved as part of a larger regional and collaborative NG9-1-1 approach.

The extent to which any jurisdiction can address resource sharing is dependent on its willingness to share not only resources, but also dedicated control of infrastructure and operations. Existing relationships among jurisdictions may or may not support the level of cooperation and collaboration necessary to take full advantage of the technical and operational opportunities that NG9-1-1 offers. Next Generation 9-1-1 supports standardized operational models that promote resource sharing and interoperability. The nature of existing governance models and the relationships between and among jurisdictions will directly impact how, and to what extent, the NG9-1-1 model is utilized. In most cases Statutes and/or regulations may require creation or updates to allow or enable the cooperative activities envisioned by the NG9-1-1 system.

In the legacy 9-1-1 systems, PSAP managers needed fewer external relationships:

- Collaboration with other PSAPs was limited to special events or call fail-over scenarios.
- A single contractual relationship with the Local Exchange Carrier (LEC) that has typically enabled the receipt and processing of 9-1-1 calls.
- Relationships with first responders (law enforcement, fire service, emergency medical services) were relatively simple.

With migration to NG9-1-1, many more combinations and permutations of roles, relationships, and considerations are required. The following are examples:

- Service Agreements with other PSAPS and other Jurisdictions with PSAPs
- Expanded Liability issues
- Human Resources related to interconnected services
- Levels of Certification (NCMEC, Active Shooter, ADA)
- Mutual Aid agreements and MOUs
- GIS services
- Position Location providers for Emergency Responders
- Incident Management, Emergency Management
- Databases (Amber, Medical, etc.)
- Expanded Roles - enhanced interaction with Medical Community
- Video and photograph providers and technical support
- Text message service providers
- Evolution/Advances in technologies used by Police, Fire, EMS (e.g. LMR, FirstNet and others)
- New certifications

These additional relationships and the opportunities enabled by NG9-1-1 create complexity. This complexity must be managed as part of the governance model and NG9-1-1

helps. The PSAPs take full advantage of new forms of information and implement operational processes that increase overall emergency response capabilities.

Governance of the 9-1-1 service process and Public Safety Access Points (PSAPs) is currently a responsibility shared by local, regional and state governmental agencies. Demographics, funding, operational capability, and geographical location of the PSAP have contributed to the evolution of PSAP governance and its variation across the United States up to date.

The development and deployment of NG9-1-1 capable system architecture introduces additional infrastructure configurations along with new technologies and the products that will run them. Staffing, logistics, sustainment and day-to-day operations of the 9-1-1 service process and PSAPs will undoubtedly drive evolution of the governance to ensure the 9-1-1 caller continues to receive equal or greater levels of 9-1-1 dependability and reliability.

Previous FCC and other advisory groups have deliberated the governance issue within the context of possible consolidation. For example, the report of Working Group 1A of the CSRIC II (convened 2009-2011) noted, "Successful consolidations require that a trusted and secure governance structure be established, a champion must lead the project and the political leadership must be in place to support the effort." The "effective practices" related to governance found in the report, while too lengthy to include in this document, are also a valuable reference.[54]

In the technical transition to NG9-1-1, the role of the governing body must evolve. It will continue to be important for governing bodies to consider how to meet the often-unique circumstances and needs of local citizens and local responders. But as the transition to NG9-1-1 takes place, the role of governing bodies will also include balancing local needs with forming collaborative relationships to maximize the benefits that NG9-1-1 offers. By reaching across jurisdictional boundaries, there are technical, operational and financial benefits that can be realized. The TFOPA strongly encourage 9-1-1 governance bodies to explore and embrace strategies to collaborate and share resources in transitioning to NG9-1-1 as a way to meet their responsibility for providing an optimally effective and efficient emergency communications system for their citizens and emergency responders.

5.7.1.2 Moving the Sharing Process Forward

PSAP managers, 9-1-1 Authorities and their governing bodies will ultimately have to decide whether to remain independent or share resources, and are responsible for the consequences of those decisions. If they decide that for certain technical, operational or financial aspects, then there's value in working together, it will become important to establish the parameters and processes of their business relationship. It is essential to identify the person(s) that will lead the group - someone to moderate, mediate and manage that process.

The TFOPA recommends having an advocate or a champion in favor of the resource sharing process. Understanding stakeholder, agency and individual perspectives is critical when considering sharing 9-1-1 operational procedures and resources.

As jurisdictions have grappled with how to share governance, multiple models have been

[54] CSRIC II WG1A – Key Findings and Effective Practices for Public Safety Consolidation, ocs/csric/CSRIC-1A-Report.pdf" https://transition.fcc.gov/pshs/docs/csric/CSRIC-1A-Report.pdf , last accessed December 4, 2015.

considered. Citing two existing examples:

- In Michigan, considerations included:
  - A separate department within an existing department's governmental structure. This model has a civilian director who reports within the department's organizational structure with other department heads.
  - A department that is part of a participating/existing agency. Sworn personnel manage the PSAP and fall under the management of that department.
  - Independent Authority. A civilian director typically manages these agencies and reports to a board of representatives from participating members.
  - Contractual. Governmental units can enter into contractual agreements with one another in order to provide PSAP and/or dispatch service.[55]
- The Minnesota model was selected to simultaneously maximize the benefits of improved service and cost savings and minimize the concern relative to loss of control. The following were considered:
  - Separate Emergency Dispatch Department within a Participating Agency (County). The PSAP is part of the organizational structure of one of the participating entities and the PSAP is its own independent department or part of an existing department.
  - Joint Powers Structure. The PSAP is not part of any larger government structure, but is in fact an independent entity, and a commission or board is created with representatives of participating PSAPs.
  - Part of a Participating Agency (Contract Arrangement). Under this type of structure, sworn personnel often manage the PSAP and fall under the authority of the hosting agency head such as the sheriff, law enforcement, or fire chief. [56]

Resources providing guidance on shared governance are available from numerous organizations:

- Recently, NENA has (January 2016) published an "Inter-Agency Agreements Model Recommendations Information Document, describing several collaborative agreements, including templates for Memorandum of Understanding, Mutual Aid Agreement and Memorandum of Agreement. [57]
- The National 9-1-1 Program published "Guidelines for State NG9-1-1 Legislative Language" to facilitate the process of updating local and state statutes.[58]

[55] Michigan Public Safety Answering Point (PSAP) Consolidation Considerations, http://www.michigannena.org/forms/Michigan PSAP Consolidation Considerations.pdf, last accessed December 2, 2015.
[56] Minnesota Public Safety Answering Point (PSAP) Consolidation Guidebook/Resources. 2004 Report to the Legislature on PSAP Consolidation, https://dps.mn.gov/divisions/ecn/programs/9-1-1/Documents/Central_MNPSAP_Consolidation_Study10062010.pdf, last accessed August 7, 2015.
[57] NENA Inter-Agency Agreements NENA-INF-012.2-2015, rg/?page=InterAgencyAgreemnts" http://www.nena.org/?page=InterAgencyAgreemnts, last accessed August 7, 2015
[58] National 9-1-1 Program, Guidelines for State NG9-1-1 Legislative Language, " http://www.9-1-1.gov/pdf/ModelNG9-1-1legis-110812.pdf, last accessed August 7, 2015

- The National 9-1-1 Program, through a contract with the "National Conference of State Legislatures", maintains a 9-1-1 Legislation Tracking Database, which tracks state 9-1-1 legislation (introduced and enacted).[59]
- The 2015 "Emergency Communications Governance Guide for State, Local, Tribal, and Territorial Officials" is a tool for public safety professionals at all levels of government and disciplines to use in assessing, establishing, and sustaining effective emergency communications governance.[60]
- The reports for specific jurisdictions considering some form of consolidation are often publicly available as final reports presented to their governing body, and the majority of these reports contain consideration of governance models. The reader is encouraged to seek out these reports, which may be available by contacting:
  - The Association of Public Safety Communications Officials https://www.apcointl.org/
  - The National Association of State 9-1-1 Administrators http://nasna9-1-1.org/
  - The National Emergency Number Association http://www.nena.org/

5.7.1.3 The Need for Standard Data

There is a need for detailed, consistently measured, specific and well-documented data to support decisions related to how shared governance agreements will be developed and executed. These are essential in establishing clear lines of authority, roles, and financial responsibility. Attention to detail, as well as the active development of positive and ongoing relationships among all participating organizations, is necessary. The benefits of control and collaboration must be weighed and balanced by participating jurisdictions, to establish a governance model that maximizes the effectiveness and efficiency of its 9-1-1 system.

The collection and analysis of data are essential to the development of a compelling business case that supports the operation of any particular 9-1-1 model – whether the model is an independent operation or in combination with other PSAPs/9-1-1 Authorities. The analysis of standardized administrative, operational, cost and, CAD data, etc. could all be key components in substantiating decisions to operate as a single or combined entity. This is not an exhaustive list; additional data components could be added in any standardized collection and analysis. Collecting and analyzing data over time will also provide evidence of increased efficiency, effectiveness and cost savings as a result of decisions made.

While some jurisdictions collect and analyze their own 9-1-1 data, there is no single standardized data set or collection method that could serve as the basis for objective comparison among PSAPs. Creation of a uniform data system would be useful in the ongoing evaluation of individual PSAPs, and the evaluation of progress among PSAPs nationwide. Additionally metrics provide an opportunity for further analysis and to strengthen justification for targeted program funding to fill funding gaps. The National Emergency Medical Services Information

[59] National 9-1-1 Program, National Conference of State Legislatures, 9-1-1 Legislation Tracking Database, x" http://www.ncsl.org/research/telecommunications-and-information-technology/9-1-1-database-overview.aspx, last accessed August 7, 2015.
[60] The 2015 Emergency Communications Governance Guide for State, Local, Tribal, and territorial Officials. http://www.dhs.gov/safecom,

System (NEMSIS) could provide a model for a similar data system for 9-1-1.

The NEMSIS is a national effort to standardize the data collected by EMS agencies. Funded by a line item in the budget of the Office of Emergency Medical Services (EMS) at the U.S. Department of Transportation, a uniform pre-hospital EMS dataset was established, a national data dictionary was created MOUs were signed by all 56 states and territories, and a technical assistance center was established to support state implementation, and certify the compliance levels of software vendors.[61] The EMS stakeholders and software vendors were all included in this process.

As of June of 2015, 49 states & territories have implemented the NEMSIS, and standard data is collected from every EMS patient care record in those jurisdictions[62]. Local and state systems are free to collect as much data as they deem appropriate to evaluate the performance of their EMS system, and a much smaller subset of data is submitted to the national EMS database. As of June, this national database housed data from over 43 million patient care records – all available for analysis. If such a system were available for PSAPs and 9-1-1 Authorities, then valuable cost and performance data could be collected in a uniform manner, and provide essential information to substantiate decisions and any resulting improvements. For other public safety industry standards on data collection please refer to:

- https://nfirs.fema.gov/ - NFIRS – National Fire Incident Reporting System
- https://www.fbi.gov/about-us/cjis/overview - CJIS - Criminal Justice Information Services
- https://www.fbi.gov/about-us/cjis/ucr/nibrs - NIBRS - National Incident-Based Reporting System

5.7.1.4 Value Proposition

As any 9-1-1 Authority considers the evolution into the NG9-1-1 systems environment, they will need to look critically at the value proposition of any proposed strategy. A value proposition is a review and analysis of the benefits, costs, and value that an organization can deliver for the defined services it wishes to provide. It is essentially a promise of value to be delivered to stakeholders.

Questions could include, but not be limited to:

- Provides the ability to receive originating text messages and transfer misdirected text messages to other intrastate and interstate PSAPs?
- Provides the ability to transfer calls for service received via voice to other PSAPs intrastate and interstate; including call source, location, and other metadata attached to the call?
- Provides the ability to receive video and photos from a caller and transfer those video feeds and/or images to first responder in real time?
- Provides the ability to locate callers on an aggregated shared GIS platform across multiple jurisdictions?

[61] National Emergency Medical Services Information System, History of NEMSIS, http://www.nemsis.org/theProject/historyofNemsis.html, last accessed August 24, 2015
[62] National Emergency Medical Services Information System, State & Territory Version 2 Information, ateProgressReports/index.html" http://www.nemsis.org/support/stateProgressReports/index.html,

- Provides for integrated relay and other services for the deaf, hard of hearing, and other disability stakeholders?

These and other components that make up basic value propositions are being requested by 9-1-1 consumers and will need to be addressed in any migration design from legacy to NG9-1-1 PSAPs.

The NG9-1-1 decision-makers have competing priorities and limited funds. As a result, an analysis of those costs and benefits can assist in making the best implementation choice for their jurisdiction. Some of the factors in this cost benefit analysis process may include infrastructure design, quality of service, resiliency, redundancy, reliability, and operational efficiency. Best practices in these elements are in place and/or evolving.

Value proposition factors that may require critical consideration by 9-1-1 Authorities could include workforce elements, circuits and networks, core services and other infrastructure configurations, physical and cybersecurity, applications, system administration expertise, cross jurisdiction governance difficulties, and any other collection of ROI elements. Reasonable analysis would be necessary by decision-makers to determine if the cost of continuing independent operations of a 9-1-1 service, given all the required elements of NG9-1-1 configurations, has a low or high return on investment for the services required to be delivered and the risk necessary to provide those services. When both financial costs and efficiency costs exceed the risk, it may be advisable to seriously look at shared, collaborative, NG9-1-1 in any numbers of models described within this report.

Value Proposition

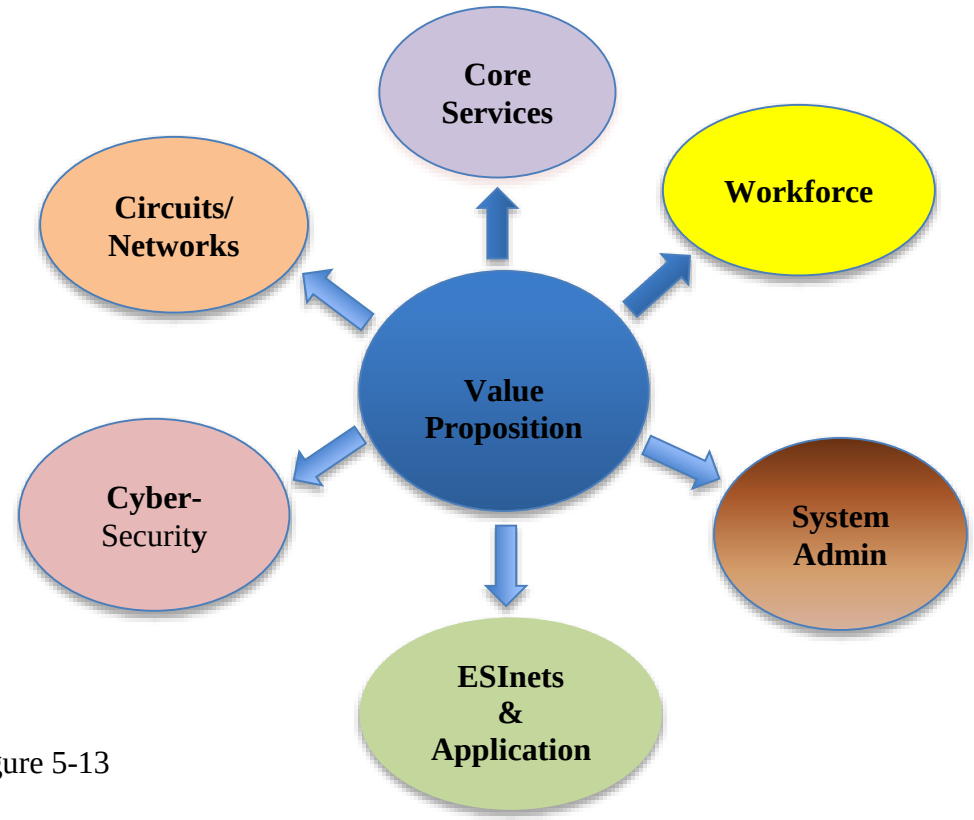


Figure 5-13

There are a number of sources available to decision-makers to frame this value proposition decision-making process. The CIO Council, Best Practices Committee developed a

"How-to Guide" that speaks to Value Measuring Methodology (VMM). The purpose of Value Measuring Methodology is to "define, capture, and measure value associated with electronic services unaccounted for in traditional Return-on-Investment (ROI) calculations, to fully account for costs, and to identify and consider risk."[63]

Financial, statutory, and intergovernmental considerations should be paramount regardless of what analytical review process is used in the value proposition. A 9-1-1 Authority (or a collection of collaborating 9-1-1 Authorities) may review a wide array of tools and potential metrics to investigate a proper value proposition. It may be reasonable for NG9-1-1 services to remain within a single 9-1-1 Authority. This possibility does not relinquish the responsibility of the single 9-1-1 Authority to forge collaborative relationships on a larger geographic scale to provide for integrated service models across 9-1-1 jurisdictional boundaries.

5.7.1.5 Financial Considerations

Financial considerations range from revenue and methods of revenue, to the cost of providing emergency communication services. Matters of revenue are addressed in greater detail in Section 6. This section will explore matters of cost, as it relates to the overall focus of this report.

In some cases, decisions related to sharing PSAP resources are directly related to cost and cost estimates. Local and state governments are charged with providing effective and efficient 9-1-1 services. The responsible stewardship of public resources includes consideration of potential cost savings, cost efficiency and value/return on investment.

Cost savings, or forecasting of cost savings, come in various forms. For example, there are many permutations of resource sharing that result in different levels of perceived cost savings. The amount of savings may vary among jurisdictions, because costs vary from one jurisdiction to another - even for the same components or processes. This makes cost comparison with other jurisdictions difficult. There is also limited NG9-1-1 savings data available. While direct comparison of cost elements may be difficult, many models have been utilized by local and state jurisdictions in considering the sharing of 9-1-1 resources, and these general models may offer a framework for others who are similar in size, capacity, or situation. Only one thing is definite – a model in which every single PSAP deploys its own independent NG9-1-1 system will be the most expensive to deploy and operate.

With NG9-1-1, every PSAP does not require its own infrastructure or core services. Whether it is GIS, translation services, cybersecurity support, or sharing of personnel and buildings, NG9-1-1 implementation further enables sharing, and raises the question of cost sharing.

In order to assess current costs, the costs of implementing NG9-1-1, and potential cost savings, it is important to define which elements are included in the definition of cost. There is not one commonly accepted definition of cost among all PSAPs. Jurisdictions may define cost by statute or by the costs they are allowed to pay for with surcharge funds. Others might include some cost elements (e.g. equipment, operational costs) and not others (i.e., personnel). Some jurisdictions could also use the calculated cost per 9-1-1 call. Whatever definition is used, it is essential to ensure that the cost elements that comprise overall cost for any single jurisdiction are standardized before they are combined or compared with those of potential collaborating jurisdictions. The Task Force recommends the TFOPA be tasked with providing additional

[63] http://www.cioindex.com/article/articleid/67467/introduction-to-value-measuring-methodology-vmm, last Accessed December 4, 2015.

research defining common elements of PSAP cost, and potential cost savings.

Once cost is defined and current sources of funding are identified and understood, it is important to establish the terms of cost sharing that collaborating jurisdictions will utilize. Making a decision on cost sharing models will be based on multiple considerations:

- Equity: What amount/proportion of total costs will each participant pay, when multiple 9-1-1 entities are working together in cooperative arrangements? Cost sharing can be based on call volume, CAD incidents, population, geographic area, property value, etc. A few examples of formulas considered, in a publicly available report out of Minnesota (referenced below):
    - Call Volume and Population Formula - percent of population within a consolidated entity, with a service delivery variable such as calls for service
    - Equal Share and Population Formula - distribute costs based on a fixed equal share, plus a proportionate share based on population.
    - Equal Share, Population, and Equalized Value Formula –

      (20% equal share + proportion of population x 80% of costs divided by 2 + proportion of equalized value x 80% of costs divided by 2 = cost share.) In this case, each participant would be charged a 20% equal share. The balance would be divided equally between each county's proportionate share of population and equalized value.
    - Equal Share, Population, Equalized Value, and Call Volume - include call volume in the formula together with equal share, population, and equalized value.

      (20% equal share + proportion of population x 80% of costs divided by 3 + proportion of equalized value x 80% of costs divided by 3 + proportion share of calls (with fire EMS calls doubled) x 80% of costs divided by 3 = cost share)

According to Minnesota's *2004 Report to the Legislature on PSAP Consolidation*,"… one of the most significant issues faced by public sector collaborations is agreement as to the cost allocation methodology. In fact, the experience within the TFOPA with consolidated operations, identified that one of the most frequent concerns of members and/or causes of dissolution is the perception of unfair cost allocation practices. Therefore, it is important to get agreement up front as to the methodology to be used for allocating costs to participants and more importantly the framework within which this methodology will be reviewed and revised."[64] Costs and savings may not be evenly distributed. It will be important for participants to understand and expect uneven costs and benefits as part of any cost-sharing plan.

The same report also lists several "Best Practices for Cost Sharing" that may be useful as jurisdictions establish roles and responsibilities related to cost sharing. For example, in selecting a cost-sharing model, it may be useful to select a model that allows additional participants to be added at a later date.

[64] https://dps.mn.gov/divisions/ecn/programs/9-1-1/Documents/mn_psap_2004_final_report.pdf, last accessed 12-4-2015

Other considerations for cost sharing models:

- The cost of sharing – cost sharing may require additional spending to facilitate the process. These additional costs may be one-time, or ongoing. Migration costs may include such items as:
- Training,
- Mechanisms to establish operational consistency,
- Extraordinary legal or legislative expenses to achieve cost sharing model,
- Connectivity,
- Support for ongoing coordination/governance,
- Harmonization of CAD, software, GIS, and
- Structural evaluations, renovations, and electrical modifications.

It is important to include additional costs in any plan, particularly to manage expectations for cost savings. Cost sharing in a traditional sense does not always result in immediate cost savings. High start-up and capital costs may delay any cost savings for several years.

- Population – any cost sharing model based on population should consider:
  - Population disbursement and density
  - Seasonal and single incident related population variances (e.g., large events) for example, Burning Man…
- Call volume - The importance of call data cannot be overestimated in providing a clear picture of the quantity of 9-1-1 service required to provide adequate coverage. The level of detail for these data is also important, and it may be useful to parse out:
  - Scalability: seasonal and single, large incident related variances in call data (e.g., sporting events, concerts, festivals)
  - Geographic areas yielding larger call volumes than others
  - Call duration
  - Types of calls – voice, text, 9-1-1 calls vs. administrative calls
- Property (Real) Value – some cost sharing models include data on property value. In this method the cost to each county is based on the assessed value of the county property. It may be important to understand that assessed value rates may not correlate well with public safety communications service requirements. Some geographic areas having low property value may generate a high number of 9-1-1 calls.

A clear advantage to combined spending is accomplished with the bargaining/purchasing clout of a larger collective entity – especially compared with the buying power of the individual PSAP. Economies of scale may result in lower costs per unit of functionality for participating jurisdictions.

Performing a cost-benefit analysis may be useful in quantifying the potential savings that could be appreciated by cost sharing. Traditional methods of cost-benefit analysis can be helpful, but the framework used by other parts of government may not be directly applicable to public safety, in terms of what is valued. The Value Measuring Methodology, utilized by the U.S. Department of Transportation's NG9-1-1 Initiative, allows the calculation of non-financial value that might not be accounted for in traditional financial metric calculations, and can provide a more rigorous comparison of alternatives, particularly in assessing the value of public safety.[65]

[65] U.S. Department of Transportation, NG9-1-1 System Initiative, Final Analysis of Cost, Value and

5.7.1.6 Statutory/Legal Considerations

No discussion of non-technical considerations would be complete without legal considerations. Since existing statutes and regulations vary widely among jurisdictions, it will be important to assess to what extent they allow the implementation of new technologies and such actions as the sharing of resources and merger of PSAP operations. Any significant differences will have to be addressed before any action can be taken toward sharing resources.

There may be implications for the resource sharing project in its entirety, or differences in how specific elements are addressed, such as:

- Employment Regulations
- Privacy laws
- Chain of evidence laws
- Liability
- Freedom of Information Act (FOIA)
- Discrepancy in procurement laws

The list of statutes, rules and regulations that govern 9-1-1 service operations are publicly available in many jurisdictions. For example, the Florida Department of Management Services Web site includes information on state statutes and the rules that pertain to their authority to function and their responsibilities.[67]

5.7.2 Intergovernmental Considerations

Historically, incumbent local exchange companies served as regulated monopoly E9-1-1 service providers within specific geographic regions. In more recent years that environment is changing with advancements in modern communications. As the historical monopoly environment is being replaced by competitive providers of interconnected network elements that may each be provided on local, regional, statewide or national scopes, the management and governance of these elements must be adapted. The ESInet and next generation core functions and services are part of that evolution.

The provisioning, use and maintenance of the NG9-1-1 system by nature requires an operational and administrative environment to insure its continuity, security and function. The nature of that environment will depend in part upon the scale of the system, along with the functions or services to be supported, and the stakeholders or customers to be served. The scale may vary from a statewide system put into place by a state-level 9-1-1 Authority or entity, to regional systems put into place by regional 9-1-1 Authorities (or groups of 9-1-1 Authorities), to

---

Risk, http://ntl.bts.gov/lib/35000/35600/35650/USDOT_NG9-1-1_4-A2_FINAL_FinalCostValueRiskAnalysis_v1-0.pdf last accessed August 8, 2015.

[66] CIO Council Best Practices Committee, Value Measuring Methodology How-To Guide, https://cio.gov/wp-content/uploads/downloads/2012/11/ValueMeasuring_Methodology_HowToGuide_Oct_2002.pdf, last accessed August 8, 2015.

[67] Florida E9-1-1 Board, E9-1-1 Legislative and Rule Resources, http://www.dms.myflorida.com/business_operations/telecommunications/enhanced_9-1-1/e9-1-1_legislative_and_rule_resources,

more local systems put into place to serve specific jurisdictional areas.[68] Combinations of the above may exist as well, and the nature of "interconnection" is a factor that must be considered.

5.7.2.1 Provisioning of the NG9-1-1 System

Logically there are three 9-1-1 Authority(s) approaches to provisioning such a system:

Managed services from a vendor may be procured to fully provide and maintain the infrastructure involved, in which case the 9-1-1 Authority is responsible for procuring and contracting for the services involved, and effectively overseeing the management of that engagement in an ongoing, operational environment;

- Functions and services may be procured incrementally, in which case the 9-1-1 Authority (or groups of 9-1-1 Authorities depending upon the scale of the system) will be responsible for procuring and overseeing multiple contractors, and insuring that their services interoperate effectively together in a cohesive and productive matter;[69]
- The 9-1-1 Authority or groups of 9-1-1 Authorities may elect to retain the services of a third party "multi-sourcing service integrator" to manage and oversee the incremental approach, in which case the 9-1-1 Authority is responsible for managing that engagement.

What procurement approach works best for a 9-1-1 Authority will depend in part upon historical governmental and institutional relationships, the nature and scope of the statutory environment involved, and other system goals and needs. In any of these cases, service concerns will be similar, and will revolve around interests like:

- Incident, problem, change, and configuration management, along with request management and fulfillment
- Service delivery services, including, but not limited to matters of availability, capacity, service level, continuity, security and service component management and coordination
- Equipment and Software Services, as appropriate, including, but not limited to things like long range planning, evaluation and testing, services and products being delivered
- Finance and budgeting

Other administrative/operational considerations include:

- General project management and support
- Project planning, as new projects emerge
- Resource allocation and management
- Vendor management and coordination
- Quality assurance
- Documentation
- Crisis management
- Training and education

If the ESInet involved supports other emergency services beyond NG9-1-1 core

Last accessed September 3, 2015.

[68] This potentially could include formalized interlocal arrangements of 9-1-1 Authorities serving an entire state.

[69] For example, 9-1-1 Authorities may elect to procure duplicative infrastructure from more than one vendor to augment network robustness and redundancy.

functions, then other stakeholders are likely to be involved, with their own set of functional requirements and interests that must also be accommodated in the context of the above.[70]

5.7.2.2 9-1-1 Authorities

NENA describes a "9-1-1 Authority" as a

> *. . . State, County, Regional or other governmental entity responsible for 9-1-1 service operations. For example, this could be a county/parish or city government, a special 9-1-1 or Emergency Communications District, a Council of Governments or other similar body.*[71]

In the context of this discussion, a 9-1-1 Authority could be a PSAP host governmental agency that is directly responsible for the dispatch of emergency response services (e.g., a municipality or a county), or a separate entity that is not directly responsible for emergency response, but oversees the planning and coordination of 9-1-1 for a defined geographic region (e.g., an emergency communications district or council of governments). Often such special purpose entities also provide funding and supportive services to multiple PSAP host governmental agencies.[72] Such institutional environments will impact the governmental and administrative arrangements necessary for NG9-1-1.

5.7.2.2.1 Single 9-1-1 Authority

If a single 9-1-1 Authority desires to provision a NG9-1-1 system, then governance, oversight and operation of the system is logically the responsibility of that entity. Such an authority could be a unit of state government with statewide jurisdiction, or a sub-state authority responsible for a defined geographic area as described above. If the latter, and, if said authority is also a PSAP host governmental agency, then decisions regarding the scope and nature of provisioning will logically be limited to that entity.[73]

On the other hand, it is likely that NG9-1-1 will foster broader geographic arrangements requiring systems serving multiple PSAP host governmental entities – arrangements that would maximize the opportunity for infrastructure sharing and interoperability. That opportunity fits well with state and regional 9-1-1 Authorities that already support 9-1-1 services in larger geographic areas. Such entities are likely to already have in place governmental and administrative arrangements with their PSAP host governmental customers that can serve as a starting point for the migration to NG9-1-1.

On the other hand, the nature of NG9-1-1 potentially involves a different kind of relationship with served PSAPs. The nature of support that a 9-1-1 Authority provides its PSAP customers may change to include, for example, ESInet and NGCS provisioning – infrastructure

---

[70] An ESInet broadly not only provides a network infrastructure environment for "emergency services," including 9-1-1 services, but also potentially including broader public safety services like first responder communications, emergency preparedness, homeland security, and similar functions. The scale of an ESInet may be a large geographic area depending upon the services involved, and the interconnectivity desired. Different functional software environments may be operated by different stakeholders (e.g., supporting applications for functions other than 9-1-1, etc.)

[71] "NENA Master Glossary of 9-1-1 Terminology," National Emergency Number Association (NENA), NENA-ADM-000.18-2014, 07/29/2014, p 18.

[72] For example, database services, network infrastructure, call-handling equipment, maintenance, etc.

[73] Recognizing that the need for interoperability with neighboring governments will necessarily involve varying degrees of joint coordination and planning.

over which, by definition, 9-1-1 calls will be delivered utilizing new IP based technology. That is likely to generate new matters of policy and operational management involving both the procuring agency (i.e., the 9-1-1 Authority) and user agencies (i.e., the PSAPs).[74]

Governmental and administrative mechanisms structured around policy and operational matters may need to be put into place to insure the appropriate involvement and input from all relevant stakeholders. For a single 9-1-1 Authority, the policy side of that may already be adequately addressed by nature of the authority's structure. However, it is likely that new or enhanced operational mechanisms will need to be developed to deal with the nature of NG9-1-1 and changing roles and services.

5.7.2.2.2 Multiple 9-1-1 Authority Arrangements

Next Generation 9-1-1 is being designed to support an interconnected system of local, regional and state emergency services networks. Effective interconnection requires effective planning and coordination, and will be based upon a variety of factors, including, but not limited to local, regional and state emergency event response considerations, historical institutional, statutory, and geo-political cultural arrangements, existing and desired joint service environments, and resource sharing opportunities, factors and constraints.

Reconciling all of those factors may suggest NG9-1-1 systems beyond the scale of a single 9-1-1 Authority region. When that occurs, multiple 9-1-1 Authorities may be engaged, and new intergovernmental arrangements must be developed to oversee the service environment desired – arrangements that provide a fair and equal role for all the 9-1-1 Authority stakeholders involved. Many if not most states have statutes in place to support interlocal cooperation among local governments. Texas, for example, has a section of its Government Code that specifically is designed ". . . to increase the efficiency and effectiveness of local governments by authorizing them to contract, to the greatest possible extent, with one another and with agencies of the state."[75] Florida has their "Interlocal Cooperation Act of 1969." Generally, such statutory authority allows local governments to enter into arrangements together to perform any governmental function or service that each entity is authorized to perform individually.[76] The Florida Act ". . . authorizes local government units to enter into interlocal service agreements either with the public or private sector. Florida's Interlocal Cooperation Act reflects also a general law allowing a mix in the approaches adopted to deliver services, which has led to extensive use of interlocal service agreements by counties in Florida."[77]

There are many examples of these kinds of arrangements. One of the better ones is the Greater Austin Area Telecommunications Network (GAATN) in Texas that exists through the above statute and provides fiber optic connections to member agencies to support

---

[74] For example, security and access management, data sourcing and maintenance, domain name service (DNS) and IP addressing management, network logging, voice recording, network operations and software support, etc.

[75] Texas Government Code, Title 7. Intergovernmental Relations. Chapter 791, Interlocal Cooperation Contracts. Sub chapter A. General Provisions.

[76] There is a long history of local governments working together in different ways to provide joint services. For example, A Wayne State University study on "Interlocal Contractual Arrangements in the Provision of Public Safety" identified ". . . 2,251 different types of contractual arrangements in the provision of public safety." Andrew, Simon A., "Interlocal Contractual Arrangements in the Provision of Public Safety" (2005).Working Group on Interlocal Services Cooperation. Paper 6. http://digitalcommons.wayne.edu/interlocal_coop/6 last accessed December 2, 2015

[77] Andrew, ibid. p10.

communications services.[78] Members include the Austin Independent School District, Austin Community College, City of Austin, Lower Colorado River Authority, Travis County, the State of Texas, and the University of Texas. The GAATN provides a variety of networking technologies to its members, including support for emergency notification and high speed backbone network infrastructure to transmit GIS data for emergency service delivery.

The GAATN has a Board of Directors composed of members from each member entity that provides policy oversight over the operations and services of the network. A "Technical Subcommittee" is appointed by the Board to plan, review and make technical recommendations to the Board. The Board in turn solicits proposals to network maintenance, management, legal services, insurance, and other related matters. Costs are shared by terms of the agreement.

The GAATN, by nature, is an intergovernmental governance arrangement created to support specific services beneficial to all its members. Similar arrangements can be utilized, as appropriate, to support ESInets and NG9-1-1 systems serving larger scale geographic areas when the optimal service paradigms call for it. In such cases, the interlocal arrangement oversees the procurement, deployment and operations of the ESInet.[79] There is no set size to such arrangements. It depends on needs and the factors describe above. And, such arrangements may enter into agreements with similar organizations to insure interoperability.[80]

5.7.3 Collaboration to Promote System Reliability and Continuity

The transition to IP-based technologies and the standardized architecture developed to support NG9-1-1 are explicitly designed to promote a diverse public / private ecosystem that will increase innovation, reliability, and competition, and enhance the functionality and utility of 9-1-1 services, and these principles should be promoted.

Efforts should be made to accelerate the continued development and implementation of NG9-1-1 standards and systems, while assuring reliability (including where systems serve diverse geographic areas). Federal, state, regional, and local authorities, as well as 9-1-1 service providers and other providers, have existing roles and responsibilities to meet increased consumer expectations for reliable 9-1-1 services which span 9-1-1 coordination, operations and governance. The migration to NG9-1-1 compels the entire emergency communications industry to evaluate whether and how these roles are changing, including the appropriate demarcation points between networks used to access NG9-1-1 services and the actual NG9-1-1 services provided by 9-1-1 service providers. Increased clarity on these issues will help to reduce potential delays in NG9-1-1 deployment.

Migration to NG9-1-1 provides the opportunity for PSAPs and jurisdictions to share resources at a level not possible in the legacy environment. It also raises the question of whether or not resource sharing should be considered such as technical or nontechnical resources, virtual sharing or sharing of brick and mortar. All deliberation will include discussion of the exact nature of how all relevant stakeholders will relate to each other – governance. The nature of

[78] For more information about GAATN, see: https://www.gaatn.org/index.php Last accessed December 2, 2015.
[79] There is a lot of flexibility in how such arrangements operate. For example, individual members can be assigned or assume specific responsibilities for which they may be uniquely qualified.
[80] Ultimately such mechanisms can be used to support statewide NG9-1-1 services, including functions like state-level "forest guides" that help route emergency calls to the most appropriate serving NG9-1-1 system. Such guides keep track of the geographic coverage of the system in a state.

existing governance models, and the relationships between and among jurisdictions, will directly impact how, and to what extent, the NG9-1-1 model is deployed and the extent to which their citizens will realize its benefits.

5.8 NG9-1-1 Planning and Transition Considerations

5.8.1 NG9-1-1 Transition

The movement toward nationwide NG9-1-1 continues to be an evolving process. Most PSAPs continue to function in 'Legacy 9-1-1' configurations, a number can be considered to be 'Transitional', but as of the time of this report no 9-1-1 Authority has attained a 'Fully Functional NG9-1-1' implementation. As described above, Legacy PSAPs continue to operate in a TDM central office switched environment and have not moved toward the necessary IP environment with core service elements for NG9-1-1.

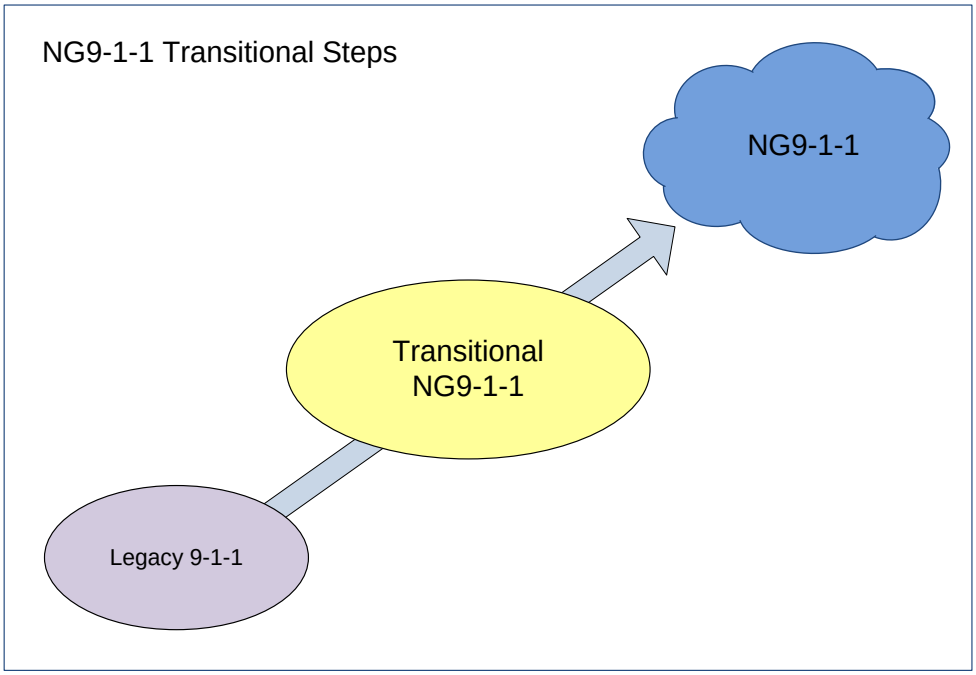


Figure 5-14

The end state NG9-1-1 is illustrated in Figure 8-2. The operating domains, OSEs, NG9-1-1 Core Services Providers, and PSAPs operate together to provide complete 9-1-1 services. OSEs deliver "calls" to NG9-1-1 Core Services Providers who route those requests for assistance to the proper PSAPs. These operating domains are interconnected via the ESInet, which provides IP transport and other networking services. The capabilities of OSEs are expected to change over time as Access Network Providers and Communication Service Providers evolve their products and capabilities. New emergency service features will also be introduced into the overall NG9-1-1 System Services Environment.

Figure 5-15

Ultimately, 9-1-1 Authorities need to make decisions necessary to begin the transition process. In most cases, these governance decisions will not be made by single PSAP Authorities even though those PSAP Authorities may currently have self-contained legacy 9-1-1 systems. Instead, new coalitions and collaborations of cooperative PSAP Authorities, at various levels, will need to evolve and work together to achieve economies of scale. These new 9-1-1 Authorities will emerge at the state and/or multi-jurisdictional levels, as discussed in previous sections of this report.

The evolution strategy from legacy 9-1-1 to NG9-1-1 is critical to 9-1-1 Authorities due to the complexities involved and costs imposed by duplication. Conversion delays, which create a combined legacy network and NG9-1-1 architecture, will require funding overlapping systems. It is inevitable that not all PSAPs will have the advantage of migrating to a NG9-1-1 environment at the exact same time. There will be early adopters and those delayed for a variety of reasons. The 9-1-1 Authority will bear larger costs while the two-system hybrid architecture remains in place. Also, PSAPs will not have the full advantages offered by an integrated NG9-1-1 environment, such as multi-media information exchange between PSAPs, while the hybrid environment exists and sets of PSAPs are served by different systems. Therefore, it is recommended that 9-1-1 Authorities explore transition strategies which reasonably minimize duplication.

Figure 8-3 below illustrates a dual environment where the legacy Selective Router is maintained and PSAPs are served by either the legacy Selective Router or NG9-1-1 Core Services. A common industry transition strategy is to deploy the ESInet, with either IP Selective Router functions or NG9-1-1 Core Services, and connect to PSAPs but leave the legacy Selective Router in place. This deployment strategy allows PSAPs to connect to the ESInet without the added complexity of trying to work with a variety of OSP/OSE to “re-home” their ingress traffic. After PSAPs are fully connected and receiving calls from the NG9-1-1 Core Services, the legacy Selective Routers can be removed from the call path for those PSAPs converted. However, legacy Selective Routers may serve more than the PSAPs migrating, therefore, the legacy Selective Router will be required to remain in service until all PSAPs have migrated to NG9-1-1 Core Services. This may require additional costs to all the PSAPs served by that legacy Selective Router and those still served by that legacy Selective Router.

Dual Legacy and NG9-1-1 Environment

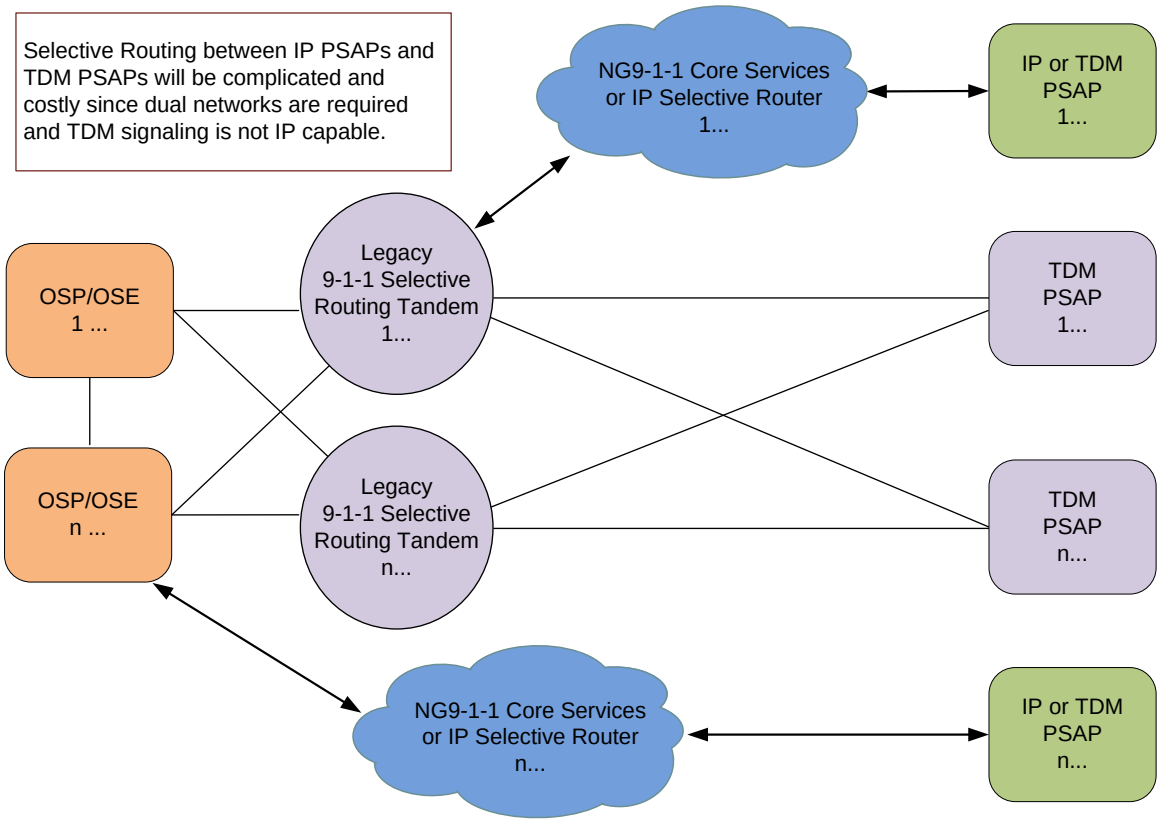


Figure 5-16

In NG9-1-1 configurations, through the establishment of Emergency Services IP networks, NG9-1-1 Core Services can reside anywhere on the network and can be economically shared in collaborative environments as depicted below. An important understanding in this transition planning process will be for the 9-1-1 Authority to have a true appreciation for what is involved in the NG9-1-1 ecosystem from a technology and functionality position.

Transitional NG9-1-1

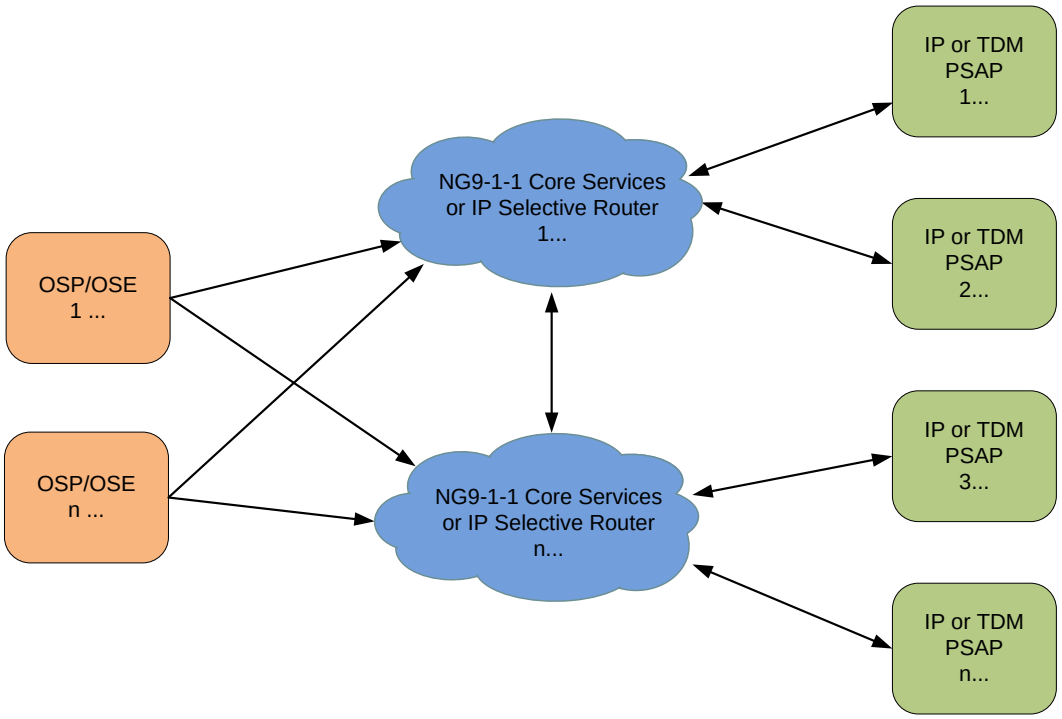


Figure 5-17

The 9-1-1 Authorities should develop an in-depth NG9-1-1 transition plan. With proper planning, NG9-1-1 Core Services, as described in this report, can be implemented in a reasonable time frame. Through economies of scale 9-1-1 Authorities can minimize transitional costs and maintain positive outcomes with maximum fiscal responsibility.

The 9-1-1 Authorities need to develop an understanding of the steps appropriate for them and their specific situation. Figure 8-5 below suggests that there are three primary capabilities or "Foundation Elements" that must be established to achieve NG9-1-1. These elements, ESInet, IP PSAP and GIS Data Preparation, do not necessarily need to be accomplished simultaneously or in any particular order, but completion will be driven by the 9-1-1 Authorities goals and NG9-1-1 transition plan. The 9-1-1 Authority's planning and ability to fund the various stages of system development and implementation will determine the following timeline.

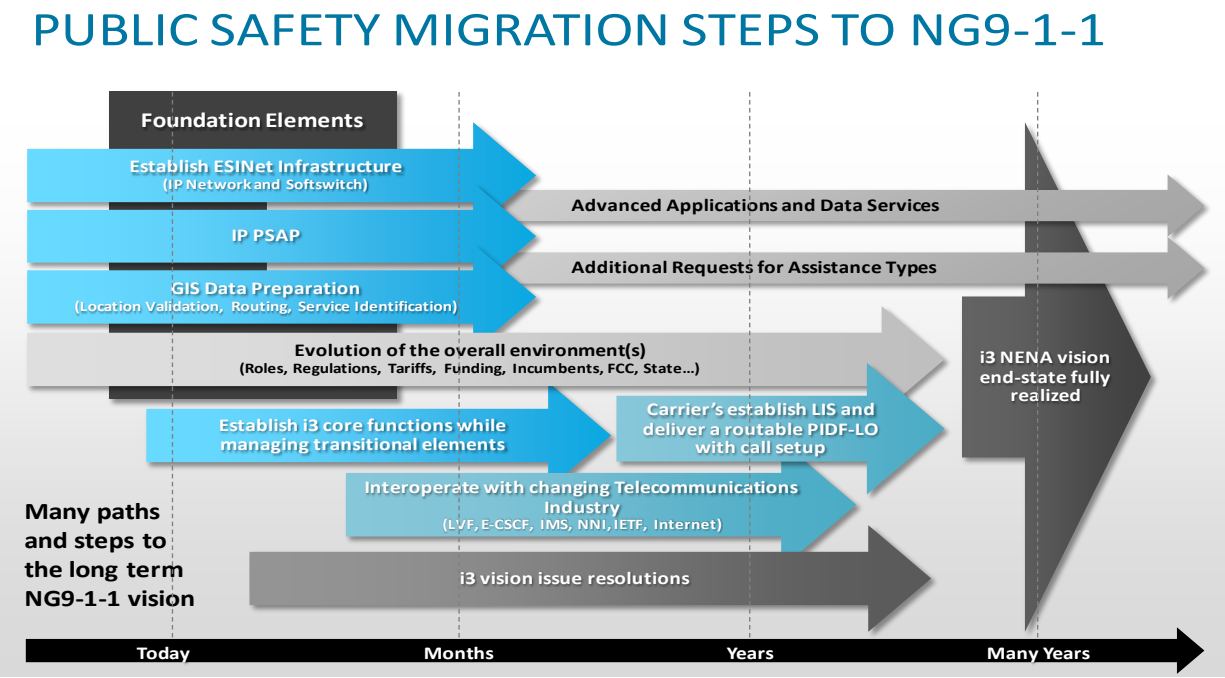


Figure 5-18

With NG9-1-1 configurations, 9-1-1 Authorities need to examine all of the considerations discussed in the previous Sections of this report to determine the optimal arrangements for their particular circumstances. To support this planning, the 9-1-1 Authority needs to consider the baseline features and functions as described in this report and determine their migration to NG9-1-1. The table below describes baseline features and functions according to the most recent NENA standards.

Function	Transitional NG9-1-1	Full NG9-1-1	Notes
Base Transport Network	ESInet	ESInet	Emergency Services IP network
Traditional OSP Access	LNG, LSRG	Multimedia IP interface	IP such as IMS ESInet
Other OSP Access	Multimedia IP interface	Multimedia IP interface	
Location Validation	LVF/GIS or MSAG equiv	LVF/GIS	LVF can be internal or external
Primary Routing	ECRF/ESRP	ECRF/ESRP	GIS controlled in both
Policy Routing	Base PRF equivalent	PRF	
Geospatial DB	GIS	GIS	

Primary Data Access	ALI, MPC, VPC, etc.	LIS, CIDB and variants	
Additional Data Access via NG9-1-1 core system	Maybe	Yes	
National and State ECRFs	No	Yes	Forest Guide process
Call transfer w added data	Maybe	Yes	
Interoperability w other NG9-1-1 systems	Maybe	Yes	Requires ESInet Interconnection
Full NG9-1-1 monitoring/logging	Partial	Yes	
PSAP interface	LPG or IP	IP interface	Legacy or NG capable PSAP

Source: NENA – see also the Baseline NG9-1-1 Description. [81]

The NENA Baseline NG9-1-1 is a description of a basic set of features & functions that constitute a NENA Standards based NG9-1-1 solution, on the path to an end-state NENA i3 architecture. The NENA i3 architecture components are only one aspect of NG9-1-1. There are more components that make up a complete NG9-1-1 "system", such as fully NG9-1-1 compliant PSAP equipment and the provision of GIS data. As future needs are identified, overall NG9-1-1 standards will be updated.

In order to be fully compliant with NENA NG9-1-1, the baseline NG9-1-1 system must include the functions of the legacy E9-1-1 system replicated in IP technologies as defined by NENA NG9-1-1 Standards. This includes all network and PSAP components of the system and a number of capabilities beyond E9-1-1 functions, such as the basic ability to support non-voice multimedia, e.g., text and video. While these forms of communication may not be immediately available through traditional originating service providers, baseline NG9-1-1 has the system functionality to support multimedia, perform routing, provide for call media logging, and enable PSAP/caller interactive communications (voice & non-voice).

Therefore, as originating service provider IP based standards are finalized and aligned with NENA NG9-1-1 standards, disruptive software application or hardware changes are not expected in NG9-1-1 systems.

Minimally required components or capabilities of baseline NG9-1-1 include, but are not limited to:

1. ESInet (Emergency Service IP transport network)

[81] http://www.nena.org/?NG9-1-1_Baseline last accessed December 2, 2015

2. GIS data creation to support components 3 and 6 below, and associated management tools

3. Location information validation functions (LVF)
   Publication of Authoritative NG9-1-1 Validation Functions for use by OSEs to pre-validate civic addresses (in replacement of MSAG).

4. Publication of Authoritative NG9-1-1 Routing Data for 9-1-1 Authorities. This Boundary data is loaded into ECRF and Forest Guide functions.

5. Support for legacy originating services via gateways (e.g., Legacy Network Gateways, Legacy SR Gateway), including access to MPCs, VPCs, and traditional ALI databases)

6. Geospatial controlled call routing functions (ECRF and ESRP)

7. The ability to control call routing based upon a policy routing function (PRF) with standardized methods to define/build and control Policy Rules

8. Additional data acquisition after call delivery via NG9-1-1 core services to facilitate call processing by calltaker or other public safety entities, including wireless location information rebid

9. Support for transfer of calls with accumulated calltaker notes and added data, or an access key to such data, to any authorized entity interconnected by ESInets

10. Ability to interconnect with other NG9-1-1 systems and to interwork with E9-1-1 systems

11. Support for system monitoring/logging/discrepancy reporting necessary to support troubleshooting and ongoing operation and maintenance

The above minimally required components or capabilities of baseline NG9-1-1 must include architectural, security, confidentiality, interconnection with other 9-1-1 systems, and operations aspects of NG9-1-1 service as defined in NENA Standards and related documentation. The use of legacy PSAP software through legacy PSAP Gateways will limit PSAP access to NG9-1-1 features. Fully capable NG9-1-1 PSAPs can make full use of NG9-1-1 Core Services.

The following is an example progression chart that illustrates the planning path to NG9-1-1 from legacy TDM.

NG9-1-1 Deployment Progression Chart

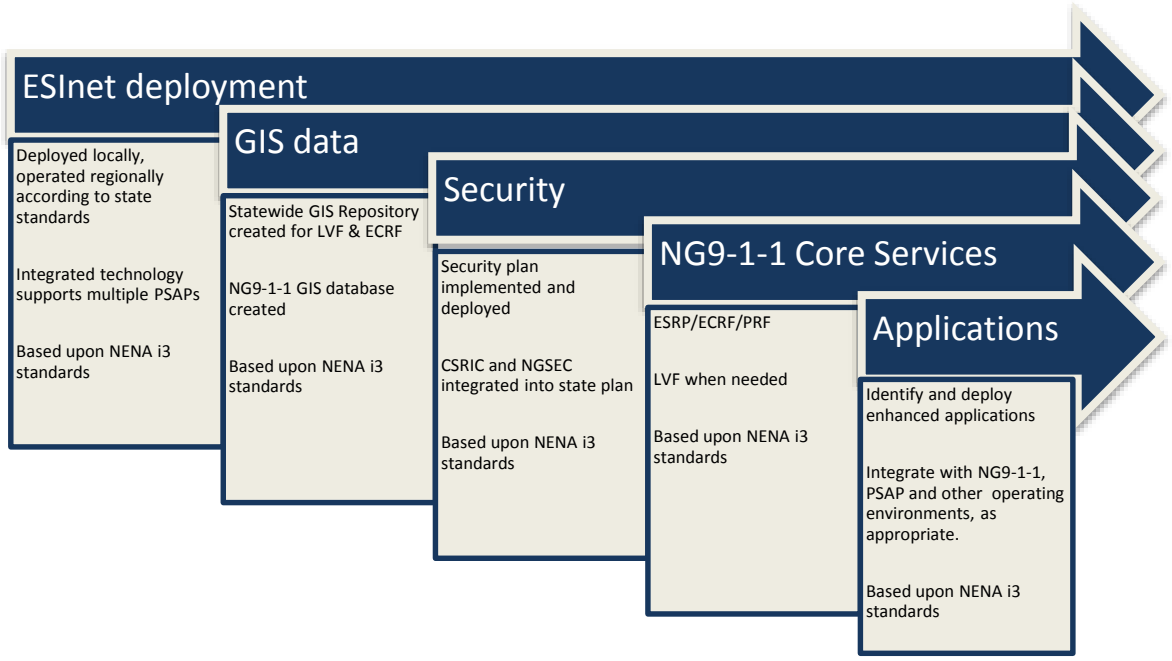


Figure 5-19

The PSAPs should work with their 9-1-1 Authority to create an overall plan and progression chart for their particular situation. In cases where there is no established 9-1-1 Authority, PSAPs should first address their organizational approach and financial capabilities to move forward. A plan should include the basic migration steps explained above and move toward the more detailed functional capabilities and functional elements. 9-1-1 Authorities should continue to monitor industry standards organizations to ensure they stay abreast of best practices and industry directions.

5.9 Summary, Recommendations, and Conclusion

5.9.1 Summary

Historically, the public safety community has faced numerous transitions and enhancements to newer, better, faster, technologies that are used to support the delivery of services. These transitions, migrations and adoptions often come with complexities and consternations.

The evolution and eventual transition of 9-1-1 services to NG9-1-1 technology is similar to the continuing digitalization of land mobile radio services and the adoption of Project 25 (P25) standards based technologies that have been ongoing for the past 30+ years. With P25, the technology of public safety radio took a giant leap forward with the move to digital protocols for radio. This has not come easily as it required substantial education and understanding of the fundamental changes of how this new technology could be applied and support operations with a myriad of new features, functionality, and capabilities. The advent of FirstNet and the envisioned move of public safety wireless/mobile data services to Long Term Evolution (LTE) technology represent another similar technology migration and provide an opportunity for a holistic approach to emergency communications as an enterprise.

Generally, the items below are fundamental considerations that should be identified, addressed, and researched to satisfy the concerns of fitness and readiness of the identified technology to support critical public safety services. As this document illustrates, the aspects of transitioning 9-1-1 services from the current legacy environment to the NG9-1-1 environment will present a myriad of technical, operational, and political choices for governments and the public safety community at all levels. Some of the overarching elements are categorized and presented below.

5.9.1.1 Governance and Policy

As NG9-1-1 accelerates and matures, current roles and responsibilities among all entities involved in providing 9-1-1 services will be impacted by the impending technology choices and changes. As is common with the evolution of technology, existing legal and regulatory environments will be reactive and will not always effectively accommodate their implementation.

The deployments of NG9-1-1 will require increased coordination and partnerships among governments and public safety stakeholders at all levels. This includes 9-1-1 PSAP administrators, service providers, carriers, services and equipment providers, in order to collaborate and coordinate research and planning functions to ensure that the selected approach for a given PSAP or 9-1-1 Authority, is indeed the most appropriate implementation of the NG9-1-1 infrastructure. The selection, development, and ultimate implementation of the new NG9-1-1 infrastructure will often require personnel with differing skill sets and modification of service roles and responsibilities.

Effective communications and coordination with political and public safety agency leadership and the general public will be important in addressing concerns and managing expectations. As a result, both legislative and regulatory arrangements at all levels of government that extend oversight into the 9-1-1 environment may require reexamination and some existing statues, policies, rules and regulation will certainly require modification in order to effectively support NG9-1-1 implementations.

5.9.1.2 Operational Considerations

In order to realize the true potential of NG9-1-1 technologies, the operations of the nation's 9-1-1 systems at multiple levels will undergo significant changes and benefit from a multitude of additional capabilities to enhance the receipt and processing of citizens' calls for public safety services.

While combinations or consolidations of PSAPs, may appear as an advantageous alternative during the transition to NG9-1-1 technologies, the decision to do so requires significant analysis and reflection to ensure that the best decision is made based on the overall needs of the affected stakeholders. Transitions to NG9-1-1 technologies do not inherently require that PSAPs undergo a combination or consolidation of facilities as the technology is highly flexible and as illustrated herein offers many deployment choices. The NG9-1-1 technology decision should be premised primarily upon what is the best manner and method for the 9-1-1 Ecosystem to deliver public safety call receipt and processing services to the citizenry and the public safety response agencies.

The roles, responsibilities, and expectations of 9-1-1 personnel will change dramatically with the additional communications pathways that will be afforded to the citizenry to contact

PSAPs for public safety services. There will be an increased quantity of available multimedia information that will enhance and expand existing call handling and processing functions. The existence and application of this expanded information should allow for better and more informed decision processes and subsequently better and more appropriate responses of public safety field resources. The safety of citizens and public safety personnel should be enhanced through the implementation of NG9-1-1 services.

However, the existence and accessibility of more information surrounding a call for services or an ongoing incident may also create elongated processing of 9-1-1 calls, increase the workload of the call takers and Telecommunicators, and as more NG9-1-1 capabilities are introduced, significantly change the calltaker/Telecommunicator's experience through available visual media in addition to audio, text, and additional data information. Alternatively, there may well be situations in which the implementation of NG9-1-1 services and systems will save significant time in the receipt, processing and dispatching of calls for service.

The implementation of NG9-1-1 technology will require significant training, re-training and recurring supplemental training and education through the transition into the end state of the technology implementation. This training will be limited not only to PSAP personnel, but also should include personnel from those public safety agencies that receive services from the PSAP. Government officials and agency leadership should be provided overview training and education to further understanding and gain champions and buy-in through the transition into the end state of the implementation.

The 9-1-1 PSAP communities will incur more expansive operational responsibilities with the implementation of NG9-1-1 technologies. PSAP leadership and technical staffs will be responsible for managing a significantly more complex and connected network infrastructure. This will include the challenges of managing a broader set of shared resources, (e.g. CAD, RMS, alarms, alert & warning systems, video monitoring, telephony systems, etc.) which facilitate the delivery of multi-discipline public safety responses.

The transition to NG9-1-1 technologies assumes that PSAPs are likely starting with an environment consisting of traditional E9-1-1 components such as an ALI system, selective router(s), a Database Management System (DBMS), tabular MSAG, and a legacy 9-1-1 network. It also assumes that PSAPs have developed a set of GIS data to a level of granularity that approximates the contents of the tabular MSAG. Furthermore, it assumes that PSAPs and/or 9-1-1 Authorities that are using GIS have previously performed preliminary reconciliation between their GIS data and their MSAGs. This is essential to provision the NG9-1-1 technology GIS based Location Validation Function (LVF) and Emergency Call Routing Function (ECRF). If this is not the case, then the preparatory work for PSAPs and/or 9-1-1 Authorities to implement NG9-1-1 services will be substantially elongated as the technology is dependent upon the foundational GIS elements of street centerlines, PSAP boundary, public safety services boundaries, and authoritative boundaries. Also, if PSAPs and/or 9-1-1 Authorities using GIS have not performed reconciliation work between their GIS and US postal service address data, then this work should be undertaken as soon as practical. This is considered one of the first steps in NG9-1-1 data transition. .

5.9.1.3 Technology Standards

Adherence to accredited technical standards and accepted technical specifications is of fundamental importance and essential to the end state implementation of NG9-1-1 technologies. The use of standards and industry accepted specifications promotes and enhances data and

systems interoperability on a nationwide scale among the geographically dispersed 9-1-1 systems and public safety response agencies. The foundation of NG9-1-1 is an interconnected system architecture that incorporates a plethora of different technical standards and specifications to support the operational requirements of the network components and services in the IP world. Currently, a collection of telecommunications, networking, and telephony standards and specifications that impact and delineate NG9-1-1 networks, components and services have been developed with many others still in process. As these standards and specifications evolve, so too will the path to NG9-1-1 implementation.

Public safety and industry standards development organizations have arrived at a consensus regarding the technical architecture of NG9-1-1 systems which builds upon the capabilities and benefits of the industry-recognized and accepted deployments of IP enabled network and internetworking environments. Standards and specifications are dynamic and their development takes into account compatibilities with past and present standards to the degree that is technically feasible. As the 9-1-1 community contemplates transition and migration to NG9-1-1, they must remain aware of new and amended standards and specifications that may impact the development, planning, and implementation of NG9-1-1. While baseline technology standards and specifications have been developed, degrees of uncertainty remain among 9-1-1 decision-makers, public safety agencies, and service and equipment providers which may hinder near term transitions to NG9-1-1 technology.

5.9.2 Findings and Considerations

This work is not exhaustive. Additional guidance needs to be developed to best make use of this information, and the TFOPA encourages the Federal Communications Commission to charter such efforts as part of the 2016 TFOPA initiative. Potential topics to be explored could be the potential costs of transition, comparative early developer use cases, additional study of access for people with speech and hearing disabilities, and the integration of applications that provide access to the 9-1-1 system.

The TFOPA is aware that communications and communications technologies like the Internet of Things (IoT), Over The Top (OTT) Apps, analytics, and other advanced networking technologies continue to rapidly evolve and will eventually become part of the public safety ecosystem. How these technologies will affect public safety and effect how emergency response is executed in the future is a topic for potential further consideration. As the public safety technology ecosystem expands, how the new technologies and capabilities will be integrated into the NG9-1-1 environment will be an important consideration for future study and analysis.

A primary message in this report is that NG9-1-1 architecture can be customized to support almost any configuration of PSAP operations. Factors that affect these configurations include financial, political, governmental and operational considerations. An overall goal of this report is to educate 9-1-1 Authorities and policy officials so they have an understanding of NG9-1-1, its components, capabilities, deployment options, and potential benefits.

Armed with this understanding, 9-1-1 Authorities and decision-makers will be able to apply that knowledge to ongoing objective and collaborative dialogues that will enable them to craft a NG9-1-1 plan that meets the needs of their jurisdictions, ensuring all citizens including persons with disabilities have direct access to 9-1-1. As stated throughout this report, it was not the intent of the Task Force to recommend a particular configuration for the deployment of NG9-1-1, therefore this report is absent a “one-size fits all” architectural recommendation. The Task Force did feel it important to identify key “Findings and Considerations” contained in the

report that 9-1-1 Authorities might consider to assist in the planning and deployment of a NG9-1-1 system. The following represents the highlights of those considerations:

POLICY/REGULATION

- Legacy terminology is not always as precise as it needs to be; and in this transformative time in the evolution of 9-1-1, terminology that applies to NG9-1-1 should be more detailed and specific.
- Providers of 9-1-1 services must be accountable for the reliability of their services, and vendor contracts, buttressed by state-sanctioned tariffs where needed, can provide an effective means to address the availability and reliability of 9-1-1 service.
- While the transition to NG9-1-1 will bring significant benefits, it must be accomplished in a manner that does not undermine the availability, reliability, and resiliency of the 9-1-1 system.
- Consistent with existing law, regulatory policies should continue to recognize the distinction between access to the 9-1-1 system provided by Originating Service Environments and their vendors, and the 9-1-1 system itself provided by 9-1-1 System Service Providers that contract with states, regions, and local authorities for provisioning of various 9-1-1 services. As the transition to NG9-1-1 occurs, considerations should be given to whether and how the distinctions between these roles will impact overall 9-1-1 reliability. Jurisdiction in certain areas of 9-1-1 access to PSAPs is yet to be defined (e.g., applications, VoIP, etc.).
- The legacy single 9-1-1 service provider environment upon which most of the current 9-1-1 regulation was formed will need to be readdressed in the current NG9-1-1 market. Regulations that addressed needs in the legacy 9-1-1 world need to be reevaluated to determine if they are still relevant and, in some cases, may create unnecessary barriers to transition to NG9-1-1.
- Since existing statutes and regulations vary widely among jurisdictions. Therefore, it will be important to assess to what extent they allow the implementation of new technologies and optimizations such as the sharing of resources and merger of PSAP operations. Any significant differences will have to be addressed before any formal action can be taken toward sharing resources.
- Effective communications and coordination among political leaders, public safety agency leadership, and the general public will be important in addressing concerns and managing expectations of all stakeholders. In this process, both legislative and regulatory arrangements at all levels of government that extend oversight into the 9-1-1 environment may require reexamination and some existing statues, policies, rules and regulation will certainly require modification in order to effectively support NG9-1-1 implementations.

GOVERNANCE

- A national system enabling the collection and analysis of standardized administrative data, operational data, cost data and CAD data should be developed and made available to PSAPs and 9-1-1 Authorities, to provide essential information to substantiate decisions and improvements.

- Further enhancements to the governance/regulation of 9-1-1 systems and services should be developed by an advisory committee comprised of organizations such as NARUC, NASNA, NENA, APCO, and other organizations representing state, local, regional 9-1-1, and industry officials, whose recommendations would be augmented by public comment.
- Public safety agencies often contract with their 9-1-1 service providers for such services as NOC functionality and related features. Contracts should include Service Level Agreements (SLAs) and other provisions to assure service quality and reliability, which provisions will likely need to evolve in scope going forward.
- New governance structures designed to optimize the potential benefits of NG9-1-1 must be based on mutual agreement and formalized by 9-1-1 Authorities. The form of the agreement should be based on state statutes or local ordinances and should set standards for what is considered successful performance.
- The NG9-1-1 Core Services are not intended to be locally duplicated, but rather utilized as a cross-network resource in support of interoperability and backup capabilities. Additionally, it appears that regional or state level implementation of NG9-1-1 Core Services tend to be more cost effective and provide more opportunities for consistent operations and services to the public as opposed to localized implementations. As the intent of NG9-1-1 implementation is to ultimately interconnect regional, state, and national networks, it is recommended that 9-1-1 Authorities explore regional or state level NG9-1-1 Core Service implementations. Local networks of PSAPs are encouraged to integrate into Regional, State, and National Networks using a transitional plan that best fits their requirements and circumstances. However, it is understood that local regions cannot always readily implement NG9-1-1 functionality due to political, monetary, or operational limitations. The TFOPA supports region-specific transitional schedules, which may differ from one another because of the limitations mentioned above. 9-1-1 Authorities at all levels are encouraged to coordinate their planning.
- The TFOPA recommends 9-1-1 Authorities explore the use of a shared infrastructure model and embrace strategies to collaborate and share resources when transitioning to NG9-1-1 as a way to meet their responsibility for providing an optimally effective and efficient emergency communications system for their citizens and emergency responders. Having an advocate in favor of the resource sharing is critical when considering sharing 9-1-1 operational procedures and resources. Understanding stakeholder, agency and individual perspectives will be critical to the success of the program.
- There is a need for detailed, consistently measured, specific and well-documented standardized data to support decisions related to how shared governance agreements will be developed and executed. Additional research by the TFOPA is needed to define common elements of PSAP cost, and potential cost savings. Once cost is defined and current sources of funding are identified and understood, it is important to establish the terms of cost sharing that collaborating jurisdictions will utilize.

ARCHITECTUAL/TECHNICAL

- The PSAP managers and other 9-1-1 Authority leaders should start to familiarize themselves, if they haven't already, with the technologies and components that make up modern communications and data processing systems. While management personnel do not need to become technical experts, they should begin to investigate and have a basic working knowledge of technical concepts such as Internet Protocol-based networking, client/server computing, server virtualization, and cloud computing. PSAP architecture optimization will build upon the use of several of these enterprise technologies that are utilized within modern computing and communications systems including those employed in Public Safety. Managers will need to have at least a basic understanding of these technology concepts to meaningfully participate in the NG9-1-1 conversation with vendors, regulators and certain technology-savvy sectors of the general public.
- Jurisdictions/9-1-1 Authorities should analyze and consider the following factors as they evaluate the optimization models included in this report for suitability for their own unique environment. Note that this is not an exhaustive list of optimization factors but rather a list of those considered most imperative for use as model evaluation criteria by individual jurisdictions:
    - Financial
    - Interoperability
    - Survivability/Reliability (Operational)
    - Elasticity/ Scalability
    - Security
    - Operational Staffing
    - Service Operations Effectiveness
- PSAP Managers/9-1-1 Authority leaders must keep in mind that the advantages associated with infrastructure sharing only apply to those infrastructure services and functions that are actually shared. While this report covers the potential deployment models available to PSAPs and 9-1-1 Authorities, some of the models definitely involve resource and functional systems sharing across PSAPs and/or jurisdictions and their advantages (and challenges) are clearly delineated. These management teams should undertake clear, purposeful, and painstaking analyses of their individual circumstances with all of the identified advantages and challenges of each deployment model clearly in mind, so that decisions on chosen deployment models are made deliberately with full knowledge. Likewise, the continued reliance on legacy architecture should also be a deliberate choice rather than the result of "institutional inertia."
- Those responsible for NG9-1-1 systems deployment should be looking for ways to drive network interconnection across their jurisdiction and, where possible and necessary, with other jurisdictions. The use of "walled-garden" environments may have been a chosen and acceptable architecture in the past, as there were limited use cases for interconnectivity among disparate networks, but today, connectivity between networks is now more the norm than the exception. The end-state of a fully NG9-1-1 environment is a network of network. Optimization results from scale.

Optimal configurations will result from ESInets and NG9-1-1 Core services that are designed and deployed to serve populations that maximize the utilization of the networks and shared NG9-1-1 infrastructure and meet the needs of the served Public Safety Authorities.

- The TFOPA recommends that the ESInet, the NG9-1-1 Core Services functions, and controlling databases be monitored 24x7x365 by a NOC with visibility across the network. (Note that monitoring above the physical network layer may not be part of current NOC responsibilities.) All elements should be alarmed and current network and system diagrams should be available to assess any loss of connectivity or functional performance. This should include a Simple Network Management Protocol (SNMP) system to monitor the devices in the system. Priority should be established for network alarms with service impacts taking top priority. Potential service disruptions such as the loss of redundancy should also be prioritized.
- The ESInet should be secured using state of the art security technology (outlined in standards and best practice documents) that includes appliances and security practices designed to secure, monitor, detect intrusions, authenticate users, mitigate events and recover. Border Control Functions (BCF) functions, including Sessions Border Controllers (SBCs) and Firewalls as discussed in "NENA 75-001 Security for Next-Generation 9-1-1 Standard (NG-SEC)" should be employed to secure ESInet from security threats. Security requirements and practices are more thoroughly addressed within Section 4 of this report.

STANDARDS / BEST PRACTICES

- The integration and transition of end user applications into the NG9-1-1 System Infrastructure should be developed. End-user applications will be used as 9-1-1 call origination sources and may include unique interface and security aspects. An industry group is recommended to study the implications of end user application access to NG9-1-1.
- Collaboration and consensus-based forums should be used to develop and finalize voluntary best practices for providing public safety grade NG9-1-1 services. These include examining overall monitoring, reliability, notifications, and accountability in NG9-1-1 environments, which should be accomplished in an appropriate and timely manner.
    - The focus of this collaborative effort should be to develop and implement processes in the evolving NG9-1-1 environment to (1) *Identify* risks that could result in disruptions to 9-1-1 service; (2) *Protect* against such risks; (3) *Detect* future 9-1-1 outages; (4) *Respond* to such outages with remedial actions, including notification to affected 9-1-1 Authorities, and (5) *Recover* from such outages on a timely basis in cooperation with any affected subcontractors.[82] These five elements, although taken from National Institute of Standards and Technology NIST documents, have always been fundamentally applicable to overall 9-1-1 service management.
    - Recognizing that the implementation of best practices may obviate the need for additional rules beyond those adopted in the FCC's 9-1-1 Reliability Order, a

[82] http://www.nist.gov/cyberframework/index.cfm last accessed December 2, 2015.

consensus based process should recommend any changes believed to be necessary to reflect the emerging NG9-1-1 ecosystem. These recommendations should be consistent with the overarching goals of encouraging innovation and investment in NG9-1-1 and avoiding duplicative regulatory requirements.

- Best practices also should be developed for contract provisions between state and local public safety agencies and their 9-1-1 service providers to facilitate NOC functionality and other enhanced services that would promote reliability.
- As with all best practices, the collaborative work of this consensus body also should be flexible to account for differences in the financial and personnel resources available to individual PSAPs, state and local governments, and 9-1-1 Service Providers, as well as differences in the legal and governance environments in which 9-1-1 services are provided.
- Efforts should be made to accelerate the continued development and implementation of NG9-1-1 standards and systems, while assuring reliability.

EDUCATION / TRAINING

- The implementation of NG9-1-1 technology will require significant training, re-training and recurring supplemental training and education through the transition into the end state of the technology implementation. This training will not be limited not only to PSAP and 9-1-1 Authority operations personnel, but also should also include personnel from those public safety agencies that receive services from the PSAP.
- Comprehensive outreach and education for both 9-1-1 stakeholders and the public is critical to the effectiveness and overall acceptance of all aspects of NG9-1-1. The PSAPs, the public safety community, and their governmental entities must fully communicate the challenges, the needs and requirements of the envisioned transition including the identification of adequate capital and sustainment funding of the transitional and end- state NG9-1-1 technology implementation.
- PSAPs, the public safety community, services and equipment providers, policymakers, and the public need to know more about and remain informed of the impending transition to NG9-1-1 technologies and how it is impacting public safety communications and the provision of services by PSAPs. Comprehensive outreach and education for both 9-1-1 stakeholders and the public is critical to the effectiveness and overall acceptance of all aspects of NG9-1-1. The PSAPs, the public safety community, and their governmental entities must fully communicate the challenges, the needs and requirements of the envisioned transition including the identification of adequate capital and sustainment funding of the transitional and end-state NG9-1-1 technology implementation. As early adopters across the nation implement their NG9-1-1 networks and advanced capabilities, ample lessons learned and successful achievements abound and can be used to further design and implement programs, practices, and methods to successfully and effectively deploy NG9-1-1.

5.9.3 Conclusion

The infrastructure that provides 9-1-1 is undergoing rapid change and the legacy 9-1-1 infrastructure is inadequate to meet consumer communication expectations. Next Generation 9-1-1 is a continuous evolution of infrastructure and capabilities that will enhance emergency service capabilities, including ensuring and improving access to 9-1-1 for people with disabilities. It is imperative that PSAPs begin the transition from the legacy infrastructure to NG9-1-1 capabilities and consider the timeframe in which both the legacy and NG9-1-1 infrastructure will coexist. The 9-1-1 Authorities and PSAPs across the United States have different challenges and factors that must be addressed and will influence their plans for implementing NG9-1-1.

Many factors influence PSAP paths to NG9-1-1, including financial, political, government, operational and, in some cases, even the formation of a 9-1-1 Authority. There is not one specific recommended architecture model, but there are clearly advantages to groups of PSAPs sharing infrastructure and the systems that provide NG9-1-1 services. Next Generation 9-1-1 needs to move forward and it is up to governmental jurisdictions and 9-1-1 Authorities to collaboratively complete plans and develop paths forward.

6 Optimal Approach to Next-Generation 9-1-1 Resource Allocation for PSAPs

6.1 Introduction

Our nation's 9-1-1 system for emergency communications constitutes a remarkable achievement over the past half-century. It was constructed from the bottom up through the efforts of local, county and state officials in collaboration with telecommunications carriers and public safety entities. The system is grounded on an extensive "9-1-1 ecosystem" of skilled professionals at Public Safety Answering Points (PSAPs) that receive mostly voice calls and dispatch field responders to emergency conditions and events. This 9-1-1 ecosystem spawned a variety of systems, equipment, and service providers throughout the supply chain to support the existing 9-1-1 system, which is based on legacy circuit-switching service. This legacy 9-1-1 system is now also actively addressing the challenging transition to a fully-capable Internet Protocol-based service called Next Generation 9-1-1 (NG9-1-1). Moreover, it has created a "9-1-1 brand" that consumers instinctively understand and use during emergencies to save lives and property.

In fact, about 240 million calls to 9-1-1 call centers or PSAP's are made annually, or a staggering 658,000 calls per day, according to recent statistics from the National Emergency Number Association (NENA). The 9-1-1 systems are a success story of technological innovation that reflects substantial industry and government collaboration. The inherently local nature of the service is evidenced by the approximately 6,000 PSAP's deployed across the country and subject to county, municipal or regional jurisdictions. While many of these centers serve large metropolitan areas or large counties, many, are smaller or secondary offices with a small number of staff that rely primarily on the equipment and services offered by larger PSAPs. It has also provided for the education and training of thousands of locally based call takers and dispatchers – sometimes called "Telecommunicators'' – who staff PSAPs on a 24/7 basis. A critical mass of people across the country are passionate supporters of a reliable and secure 9-1-1 system that ensures public safety, whether they work at PSAP's, state agencies, telecommunications carriers, vendors, the FCC and other federal agencies.

Most importantly to our nation's citizens, the 9-1-1 system has saved countless lives and avoided millions in property damage. These systems are a classic example of a "public good" from the lens of both economics and political science. It is a public good in that 9-1-1 services provide comprehensive emergency services broadly for all citizens in distress, and those demands cannot be excluded from society. Also, competitive markets are not well suited to provide such services broadly to all who request them. Without question, 9-1-1 systems provide a crucial benefit to all of society, yet the governance and funding of the 9-1-1 system pose a challenge. Unfortunately, current methods of recovering the costs of 9-1-1 systems across multiple jurisdictions are a complex hodgepodge of approaches. Existing fee collection mechanisms are arguably outmoded. Many contend they must be updated to be more equitable, consistent, and sustainable.

Because the provision of 9-1-1 services has always been at the county or state levels, the primary funding responsibility rests with local governments. Federal agencies act as important facilitators, especially the Federal Communications Commission's (FCC's) Bureau of Public Safety and Homeland Security and the Department of Transportation (DOT)-National Highway Traffic Safety Administration's (NHTSA's) National 9-1-1 Program. In coordination with state and local governments, these federal agencies play a vital role enhancing situational awareness across jurisdictions, providing targeted, limited grant funding to PSAPs, and promoting an integrated "national vision" for NG9-1-1.

Existing fee collection systems unquestionably are under increasing strains. At the same time, many policy makers at both the federal, state and local levels are aggressively pressing to deploy NG9-1-1 systems. Some argue that current funding mechanisms are too complex and inconsistently applied across both (i) jurisdictions and (ii) the services capable of connecting callers to the 9-1-1 system. States continue to face challenges in fitting emerging services into existing funding mechanisms. Pre-paid wireless subscriptions, pre-paid wireless cards, Voice over the Internet Protocol (VoIP) technologies (nomadic, and fixed), and the OTT Internet data services have all raised such challenges. These new technologies and service allows some carriers to gain a competitive edge by avoiding paying an equitable share of 9-1-1 support. Such gaps in fee collection have forced some members of the 9-1-1 community to engage in extensive legislative battles and litigation with those non-contributing carriers whose customers still rely on the 9-1-1 system. With the advent of these new technologies, current approaches that simply assess fees on end-use device or access lines, administered largely by traditional carriers, may no longer be sufficient. Today, revenues from 9-1-1 fees imposed on wireline services continue to decrease as more households, approximately 47%, cut the cord and shift to wireless-only voice service.

The TFOPA shares the view of many in the public safety community that any technology or services capable of accessing the 9-1-1 system should contribute its fair share to operate the legacy 9-1-1 systems and also to assist in the build-out of the NG9-1-1 networks.

Other funding challenges have emerged. Some states continue to repurpose 9-1-1 fees to other "public safety purposes" or to the states' general revenue funds, both of which are inefficient and inconsistent with a State's prescription of a dedicated 9-1-1 fee. Such "diversions" are not easy to quantify without a consensus view on what actually constitutes a diversion/unrelated expenditure. But, it is clear, under any reasonable interpretation of state laws and rules that such diversions have occurred in the recent past given by state Legislatures and continue to occur in a number of states today. State and local 9-1-1 authorities and legislatures use a wide array of budgeting practices to both collect and authorize 9-1-1 expenditures. The legislative practice of sweeping uncommitted balances of 9-1-1-related accounts, especially

those intended to fund NG9-1-1 system infrastructure generally occurs quietly without much public scrutiny.

Unfortunately, such practices have delayed plans in several states to meet the deployment schedule for the transition to an NG9-1-1 system. Public safety agencies already face a period of funding dual 9-1-1 systems; the legacy circuit-switched systems based on Time Division Multiplexing as well as the new IP-based systems based on Emergency Services Internet Protocol Networks, or ESInet. These diversions of designated 9-1-1 funds will necessarily prolong any transition. This is inefficient and costly. In addition, if these trends continue, this nation may miss a unique opportunity to capitalize on the convergence of technological capabilities inherent in an IP-based architecture and system. Such capabilities have not existed in the legacy 9-1-1 networks and systems, and if the transition to NG9-1-1 is not managed and funded properly, our nation's citizens may not receive the maximum benefits from the emergency communication system. Moreover, diversions could cause gaps between the two systems that could result in unnecessary deaths or injuries or property loss, not to mention the increasing possibility of cyber intrusions or other threats that affect the reliability of 9-1-1 systems.

In short, the nation's system of 9-1-1 fee collection and expenditures is at risk. In many parts of the country, the trend lines are not encouraging. In fact, they have gotten worse over the past few budget cycles in many jurisdictions. Technologically-based "arbitrage" should not be an excuse for either consumers or providers of modern communication services to avoid paying a fair share to support NG 9-1-1 systems. The 9-1-1 community should not have to engage in inefficient legal, regulatory or statutory efforts to ensure all providers that access 9-1-1 also contribute equitably to fund the service. This report is a wake-up call to policy-makers at all levels to understand the challenges, to consider certain 9-1-1 policy principles, and to propose sustainable and technology-neutral funding solutions. This report also provides a framework for the next generation of 9-1-1 practitioners at the local and state level for fees and optimal resource allocation. The 9-1-1 community must be more proactive educating policymakers to provide a sustainable funding means for an accelerated build-out of NG9-1-1 systems. Anything less is a huge disservice to all citizens and future generations who understandably expect reliable 9-1-1 service from all modern communication technologies.

6.2 Guiding Policy Principles for any State funding Mechanism:

As NENA's 2007 *Funding 9-1-1 Into the Next Generation* accurately points out, NG9-1-1 will reflect an ecosystem comprised of shared networks, databases and application environments fostering both traditional and new types of 9-1-1 costs that must be funded.[83] In the new ecosystem, traditional stakeholders in the 9-1-1 community will work together in new and innovative ways, generating a more complex service setting that calls for the sharing of costs and financial obligations. As a matter of principle, 9-1-1 funding mechanisms should be:

- **Predictable and stable;**

  This is necessary to support budgetary planning as migration to NG9-1-1 will occur over several years and involve capital intensive projects. Revenue streams must be predictable and stable to support essential financial and budgetary planning;

[83] NENA, *Funding 9-1-1 in to the Next Generation: An Overview of NG9-1-1 Funding Model Options for Consideration* (March 2007).

- **Based on a consumer's ability to request emergency services;**

  Funding 9-1-1 service should be directed to the potential end user that such service is intended to benefit. Such a "user fee" should be based on the use of any communication service that supports requests for emergency services.

- **Reasonable, equitable and non-discriminatory;**

  9-1-1 fees assessed on end-users should be set at a reasonable rate, equitably applied and nondiscriminatory based on non-recurring and recurring costs to deploy 9-1-1 services as required by State law.

- **Assessed on all services that can access NG 9-1-1 systems;**

  This is the complement to the second principle outlined above. 9-1-1 fees should be applied to any communications service with the capability of reaching 9-1-1 public safety agencies to a request emergency services response.

- **Technologically and competitively neutral;**

  9-1-1 funding policy should support a technologically and competitively neutral service environment, and provide 9-1-1 agencies an opportunity to deploy and upgrade 9-1-1 technologies as advancements are made. Such funding mechanisms also should be flexible enough to accommodate the evolution of communication technologies.

- **Designed to assure fees can only be used to support 9-1-1 systems;**

  As a communications user fee, funding should be dedicated to the provisioning, maintenance and upgrade of emergency communication systems as defined by state statute and related state and local rules and policies. All revenues collected should be dedicated specifically for such purposes, and not diverted to other uses. 9-1-1 funds should be collected and deposited in special purpose dedicated fund/accounts held outside the legislative appropriations process and not subject to restrictions beyond the scope of the authorizing 9-1-1 legislation. Language also should be considered that prohibits the diversion of 9-1-1 funds for purposes beyond the scope of the legislation.

- **Designed to assure fair and equitable allocation of the funds collected to provide service to those that pay the fees;**

  Distribution of 9-1-1 fees should be allocated to authorized 9-1-1 stakeholders based on the relative share of cost and be distributed in a fair, consistent and equitable manner.

- **Designed to assure the revenues collected are sufficient to address transitional, provisioning and ongoing operational costs;**

  Migrating to NG9-1-1 will involve transitional, provisioning and operational costs. Any funding mechanism must be sufficient to support all three types of costs, including a combination of legacy and emerging NG9-1-1 costs during the initial stages of transition. The funding of ongoing operational costs must allow for the replacement of capital equipment and upgrades to 9-1-1 systems.

- **Clearly identified and accountable**;

  9-1-1 fees billed to end user/devices should be identified separately as a "9-1-1

Emergency Services User Fee" on consumer/user bills. Service Providers billing 9-1-1 fees should be subject to audit to ensure proper billing and remittance of the 9-1-1 fee. 9-1-1 agencies should be subject to audit.

- **Clear enough to avoid complicating the intergovernmental and sharing environment they support**.

  9-1-1 funding mechanisms shouldn't overly burden local government, and should allow for flexibility in the planning, deployment and operations of 9-1-1 systems, including intergovernmental and shared service environments.

6.3 Previous Studies

Many organizations have produced useful papers on the transition to NG9-1-1. Some specifically address funding and governance issues. While studies by the FCC and the DOT have focused on the cost of nationwide NG9-1-1 deployment, estimating the cost to range between $2.86 billion and $9 billion depending upon the chosen deployment architecture, other studies specifically address funding and governance issues.[84] [85] White papers authored by the National 9-1-1 Program of DOT/NHTSA, the FCC, NENA, NASNA, academic institutions, and others form the foundation of this report. Many are referenced in Appendix 8, Previous Studies and Analysis. Among these, the papers authored by the National 9-1-1 Program, NENA, and NASNA have been especially instructive. The March 2013 report of the National 9-1-1 Program, *Blue Ribbon Panel on 9-1-1 Funding: Current State of 9-1-1 Funding and Oversight*, provided the most recent relevant data and analysis. That paper's focus on possible NG9-1-1 funding mechanisms and the complex issues of governance and oversight provided useful background for the Task Force's discussions. NASNA's "*Four Potential Sustainable Funding Models for NG 9-1-1*" was especially useful. A draft was provided to the Task Force by NASNA leadership early in this process. NASNA approved the final version in June 2015. The paper's prioritization of the most attractive funding models was useful guidance. This study provides a summary of the pros and cons of different funding models, and highlights some challenges with implementation of any funding model. Composed of state agency officials, NASNA is both knowledgeable and sensitive to the political and economic realities of their respective government agencies. Although the TFOPA differs slightly in the analysis of the various models (e.g., on the likelihood of moving forward with the sales and use tax option), this report's recommendations are largely consistent with this NASNA study.

The TFOPA also referred extensively to the "Net 9-1-1 Reports", a report based on data that states submit voluntarily to the FCC. The FCC's Public Safety and Homeland Security Bureau (PSHSB) staff complies the information, and develops the annual report that is submitted each year to Congress. The most recent report was submitted December 31, 2014 and covers calendar year 2013. That report framed the questions assigned to the Task Force. In response, this report notes the quality and accuracy of certain data submitted by the PSAPs, 9-1-1 authorities, and states to the FCC needs to be improved and makes several

[84] "FCC Whitepaper: A Next Generation 9-1-1 Cost Study: A Basis for Public Funding Essential to Bringing a Nationwide Next Generation 9-1-1 Network to America's Communications Users and First Responders", September 2011, at https://apps.fcc.gov/edocs_public/attachmatch/DOC-309744A1.pdf
[85] U.S. Department of Transportation, Intelligent Transportation Systems, "Next Generation 9-1-1 System Initiative:
Final Analysis of Cost, Value, and Risk," March 8, 2009, pp 57-58 and 62-64, at http://www.its.dot.gov/ng9-1-1/pdf/

recommendations. This task should be a joint responsibility of the FCC and the state and local governments responsible for 9-1-1. An external audit would assist in ensuring the completeness and accuracy of this information.

NENA has also done a number of studies on NG9-1-1 related issues, including the 2007 study on funding options cited earlier. The NENA leadership and staff have been actively involved in all aspects of the NG9-1-1 architecture, governance, and funding issues. The TFOPA also found useful studies published by NENA, not specifically related to funding mechanisms, but addressing NG9-1-1 related issues, including the March, 2010 study titled *Next Generation 9-1-1 Transition Policy Implementation Handbook: A Guide for Identifying and Implementing Policies to Enable NG 9-1-1*.

Also, during the course of the deliberations, Industry Council for Emergency Response Technologies (iCERT) published a useful study by experts at Texas A&M University. Although the paper's sampling size of jurisdictions was pretty small and its analysis was broad, some of its conclusions were relevant to the financial challenge of transitioning from legacy facilities to an all-IP network. For example, it pointed out the insufficiency of capital to fund both the capital and operational needs of the NG9-1-1 systems, while at the same time operating and adequately maintaining basic 9-1-1 services through the legacy TDM systems. The TFOPA also found the work that East Carolina University College of Business, Bureau of Business Research, to be useful in the deliberations, and specifically the work that it performed for the North Carolina 9-1-1 Board.

The TFOPA also examined several State bills introduced and debated during the deliberations. It is challenging to stay abreast of state legislative efforts, and would like to recognize the diligent efforts of associations like NCSL (National Conference of State Legislatures) and the federal National 9-1-1 Program Office to keep policy makers up-to-date on emerging legislation.

During this process, the Pennsylvania legislature enacted, and the Governor signed into law a 9-1-1 governance and funding bill that, among others, set a consistent statewide 9-1-1 fee regardless of the technology used to provide the affected services. This is the right approach. Several other states, including for example, Texas, Indiana, Illinois, and Oregon, have addressed other complex issues involved in statewide and local government institutional oversight and funding. While the TFOPA lacked resources and sufficient time to follow all of these legislative efforts, it appreciates the efforts of interested groups in those states to move the agenda forward. Those efforts demonstrate that NG 9-1-1 funding mechanisms are not static. State legislatures and executive branch officials will continue to address these issues.

This report is focused specifically on implementation and execution of the recommendations rather than the broad analysis presented in the various cited reports. The TFOPA hopes these recommendations will not "sit on a shelf" while evolving communications technologies continue to overtake the ability of state funding mechanisms to keep pace. The recommendations are directed at policymakers who do not operate in the "9-1-1 ecosystem" on a daily basis, and have competing demands for their time and attention. Although no one can predict what technology will prevail in the next five-to-ten years, the 9-1-1 community must be more proactive in trying to anticipate these trends and developing a 9-1-1 funding mechanism that is sustainable and competitively neutral.

6.4 Diversion of Funding

Seven years ago, Congress asked for regular updates on potential "diversion of funding" when it passed the Net 9-1-1 Act. The TFOPA reviewed several recent reports the FCC submitted to Congress. These reports provide useful information and analysis, as well as a framework by which states and local governments can engage with the FCC on 9-1-1 issues. Still, the quality of data and analysis in these state reports submitted need improvement.

The TFOPA diligently attempted to ascertain the budgetary contexts and causes of "diversions" in the six states, and one Territory cited in the December 2014 FCC Report to Congress. However, it is very difficult to get full and accurate information on the reasons for such "diversions." State legislative processes are opaque and always state-specific. Some of these diversions have occurred for several budget cycles. Today, most state must balance its operating budget and all have faced a difficult budget environment because of the recession. What could be discovered is as follows:

California: The California Office of Emergency Services is aware of the Legislature's decision to appropriate a certain amount of funding to CAL FIRE for its use in fire protection and prevention, including dispatching crews to affected fire response areas. It appears this diversion was the result of a decision of the relevant legislative committee in a budgetary environment where resources are scarce and the needs are great.

Illinois: As noted in the Net 911 Report, Illinois is a "wireless only" collection state with no 911 fees assessed on the traditional wireline access lines. This "diversion" appears to be a long-standing practice in Illinois approved by the Legislature. The Illinois Commerce Commission (ICC) traditionally had authority over the Public Utility Fund and the Wireless Carrier Reimbursement Fund, but doesn't have the authority to transfer money from one to the other – only the Legislature can do that. For several years, as fund balances accumulated that could not be spent during a fiscal year, the Legislature passed bills that would transfer unfunded balances (from the wireless 9-1-1 fees) to both the General Fund and to the Public Utility Fund. In early December, however, the Legislature passed an appropriations bill (Public Act 099-0491, SB2039 Enrolled), signed by the Governor, which provided funding levels in three separate sections for 911 services and PSAP's, as well as funding for the State Police and administrative and other expenses. Also, this bill officially stipulated a transition for the oversight of the Wireless Service Emergency Fund from the ICC to the Illinois State Police, effective January 1, 2016.

New Jersey: The TFOPA was not able to contact anyone with direct knowledge of the alleged 9-1-1 fee diversion from legitimate 9-1-1 and NG9-1-1 purposes, to other related public safety areas such as Homeland Security and the State Patrol. Again, this appears to be the action of the relevant legislative committees to set certain priorities among the 9-1-1 community and PSAPs, relative to the needs of other state public safety agencies.

New York: The TFOPA was not able to contact anyone with direct knowledge of the alleged 9-1-1 fee diversion. The New York Public Service Commission has little direct oversight of these activities. Again, the decisions for diverting a certain amount of 9-1-1 fees appear to be made in a non-public way by the leadership of key committees and the legislature, and through the office of the Governor and key agencies related to public safety.

Puerto Rico: The TFOPA was not able to contact anyone with direct knowledge of the alleged 9-1-1 fee diversion, either in the legislative body or in the Executive Branch.

Rhode Island: As a historical and long-standing practice, the bulk of the $1.00 per access line surcharge has been deposited in the state's General Fund. Then the Legislature makes the allocations in the operating budget to the relevant departments for public safety and emergency communications. There are five relevant public laws in Rhode Island, passed by the Legislature and signed by the Governor, that govern this process during the budgeting and appropriations cycle. The Rhode Island commission has no authority over either the E9-1-1 surcharge or the approval of expenditures from such fees.

Washington State: According to state 9-1-1 officials, for state fiscal year (one year) 2014, the State E9-1-1 Fund expended $21,957,199 in support of activities related to 9-1-1 operations. Of this, $12,917,443 was expended to support the Statewide NG9-1-1 Network, state contracted 911 training resources, and the E911 Advisory Committee. However, the following activities not directly related to E911 were also funded from the 911 fees: $10,842,000 for the operations of the Washington Military Department responsible for administering the statewide 9-1-1 activities, and $3,480,000 for the Washington State Patrol. For the FY15-17 operating budget signed in to law by the Governor in July, 2015, the Military Department estimates that the Revenue Department should receive about $51 million in statewide 9-1-1 fees during the biennium. The biennial appropriations for the Military Department to manage the State E911 Program were set in law at $48,548,000. Funds for purposes other than E9-1-1 or NG9-1-1 activities in this bill directed by the Legislature totaled $12.6 million, including $8.6 million for the operations funding for the State E9-1-1 Program in the Military Department and $3.2 million for the State Patrol. However, in December, 2015, in the Governor's supplemental budget submitted to the Legislature for consideration in the 2016 session, an additional $5,679,000 was provided for "modernization of the 9-1-1 system", namely seeking to accelerate the deployment of NG911 systems in the state's PSAPs.

Some of the listed practices have been utilized for several years and have considerable inertia. However, such practices are not consistent with the goal of building out an NG9-1-1 architecture and system while maintaining the legacy 9-1-1 system. But, State law and practice must remain as the primary authority on State budgetary issues – given that states generally by law must balance their operating budgets and make difficult choices among competing priorities for scarce revenues. An overly narrow focus on "state diversions" is not particularly constructive as states make the transition to a fully-capable national NG9-1-1 system.

Instead, these issues must be challenged and addressed on a state-by-state basis based on the recommendations in this Report. There should be more transparency regarding the ultimate decisions about 9-1-1 fee revenues that Legislators and Executive Branch officials make regarding the priorities among important projects in a difficult budgetary environment. A strong education and outreach effort to those policy makers is needed, rooted in a strong partnership among federal, state, and local government agencies along with PSAP's in all jurisdictions

6.5 Potential Role of Federal Grants

The role of key federal government agencies, as stated earlier, is vital in several areas – including to help promote a "national vision" for NG9-1-1 system, addressing the "seams

issues" that cross state boundaries, providing additional oversight for any national carriers not explicitly regulated by a state (or subject to state control though contractual relations with State jurisdictional providers), and creating a sustained, credible partnership with statewide and county/municipal officials. But there is one obvious area where the federal government can play a more familiar role – targeted funding to deploy new technologies.

A. Rural Utilities Service (RUS): The TFOPA reached out to officials at the RUS to consult about potential appropriations to assist with NG9-1-1 deployments. Even if appropriations were to be provided, the actual potential and effectiveness of a loan program for NG9-1-1 is unclear. The RUS has funded electric and telecommunications capital expenditures in rural areas in the past, and it has authority to assist with public safety issues. Neither legacy nor 9-1-1 has been an active component of any RUS program.

B. Department of Justice (DOJ): The Task Force encourages the use of programs within the U.S. Department of Justice to assist in the NG9-1-1 system at state, Tribal, county, city and regional levels. This recommendation may require changes in appropriations language to designate 9-1-1 authorities as eligible entities for funding for build-out, training, standards, policy development and/or research and development.

C. FCC: The Commission, of course, is primarily a regulatory agency, and generally lacks discretionary grant funding like those residing at RUS or DOJ. Moreover, for a variety of reasons, the FCC's budgetary environment has tightened recently with the Appropriations Committees in the House and Senate.[86] This report properly focuses on potential funding alternatives to existing 9-1-1 fee mechanisms in the state and counties for both ongoing operations and maintenance, as well as capital. But the TFOPA also recognizes that potential federal funding could act as an "accelerant" with matching state funds to speed up significantly the pace of NG9-1-1 deployments.

D. More specifically, in a recent speech before an APCO conference, FCC Chairman Tom Wheeler set the stage for what could possibility be a significant step forward for NG9-1-1 deployment.[87] As this report points out as well, the Chairman noted that maintaining two 9-1-1 systems in a longer transition period is a costly endeavor for States and PSAPs around the country already strapped for sufficient revenues just to operate the current networks. The Chairman is calling on Congress to be a partner with States, PSAP's and the 9-1-1 ecosystem to facilitate a more rapid transition by: a) establish matching funds to help PSAP's migrate to efficient NG9-1-1 ESI-Nets and shared platforms; b) direct the FCC to assist states in developing effective audit tools to ensure appropriate collections and expenditure of 9-1-1 fees, and prevent the diversion of such revenue for non-9-1-1 purposes; c) establish a national maps database to ensure that every PSAP has access to the latest and most accurate data, and urge their use in PSAP operations; and d) incent the development and use of shared Security Operations Centers supporting multiple PSAP's through a shared services approach toward cybersecurity.

[86] http://www.appropriations.senate.gov/

[87] Remarks of FCC Chairman Tom Wheeler 08192015 as prepared for delivery 'Embracing Change for Public Safety Communications' APCO Conference, Washington, D.\]]]C.

E. The TFOPA notes that this Task Force is already exploring much of the Chairman's recommendations, and addressed the diversion and enhanced quality of data issues. Hence the Task Force believes that his proposals are clearly consistent with at least the recommendations of the TFOPA. Chairman Wheeler deserves great credit for opening the door for a dialogue, and for seeking to establish a collaborative approach with Congress in this area that sorely needs attention and collaborative action by the Congress, the FCC, and other federal agencies.

[1] Spectrum auctions: *The Commission may wish to seek legislative authority to authorize and appropriate some percentage of the revenues from the incentive auction for broadcasting spectrum scheduled for March, 2016 to grants for NG 9-1-1 deployment. In future auctions of spectrum, Congress should ensure that revenues in excess of the scored amount be allocated to Next Generation 9-1-1 deployment through the 9-1-1 Office. The total amount proposed for NG9-1-1 may be in the range of 2.86 billion, as cited previously. To receive Federal auction revenues for NG9-1-1 deployment, states should be required to contribute a portion of the cost through a matching grant.*

[2] Universal Service/Connect America Fund (CAF): *For the past few years, the FCC has significantly restructured the traditional federal USF support mechanisms from legacy systems, both wireline and wireless, to a mechanisms that support higher-speed broadband deployments in high-cost areas throughout the country, mainly in rural areas. The FCC is in the process of resolving issues associated with CAF Phase 2 both for price-cap carriers and traditional rate-of-return (ROR) carriers. Given the strong broadband focus in the recent restructuring of the federal USF program, the FCC should consider whether it would be appropriate and how to allocate a modest amount of funding to NG pilot programs.*

[3] Schools and Libraries Fund: *Congress created the schools and libraries fund to ensure that classrooms have broadband Internet connectivity. Congress should allow the FCC to expand the Schools and Libraries Fund to include broadband connectivity to 9-1-1 Centers.*

F. National Highway Traffic Safety Administration (NHTSA): The TFOPA also considered the incentives and disincentives (some term this the "carrot and stick") associated with NHTSA grants for NG 9-1-1 funding. In general, any federal approach solely oriented on disincentives is not constructive. Penalizing a particular PSAP in a state that has "diverted" 9-1-1 fees for other purposes, as listed in the Net 9-1-1 Report, is not helpful to either the PSAP or the cause of accelerating NG9-1-1 deployments. The PSAP in that state undoubtedly had nothing to do with the explicit decision to divert 9-1-1 fees to other purposes. In fact, a PSAP most likely advocated before the Legislature/Governor's office fighting such diversions.

The NHTSA approach should be revised and not copied by other federal programs. A more balanced approach will not only respect the concept of cooperative federalism, but also will stay focused on the ultimate goal of accelerating NG deployments. Federal agencies should remain firm in their approach toward the States that *repeatedly* decide to divert 9-1-1 fees or sweep unfunded balances for other purposes, and there should ultimately be consequences for *repeated* diversions. The following is one possible approach.

Early Warning Mechanism: Annually, the FCC, together with the NHTSA and other federal agencies, could review changes in state laws, and appropriations, that relate to the 9-1-1 funding and NG9-1-1 deployments. This is required under the Net 9-1-1 Act. But, some sort of "early warning mechanism" should be developed by the Commission and federal agencies, or through a Federal-State Advisory Committee on 9-1-1 described below, to track more effectively state legislation and activities affecting 9-1-1.

New Federal State Advisory Committee on 9-1-1: The FCC should charter a Local State Government Advisory Committee on 9-1-1 to, among other things, assess the alleged "diversions" and "sweeps of unfunded balances" of 9-1-1 fees by either Governors' Offices (through their official submittal of budgets), or key Legislative Committees and the impact on NG9-1-1 deployment.

Informal Discussions: In early stages, the federal agency staff will communicate informally with the relevant 9-1-1 authorities in each state to gauge how serious these legislative changes are. The Commission should impress on their state counterparts that there might be consequences if they proceed.

Formal Letter: At some point, if such actions are judged to be likely, the process will be escalated to the level of the Secretary's or Chairman's Office in each agency. A letter will be prepared for the signatures of the following agency heads: Secretaries of DOT, DOC, USDA, and the FCC Chair. The letter will be addressed jointly to the Governor of the affected states, and the relevant Committee Chairs in the Legislature responsible for 9-1-1 fees and expenditures. The essential content of the letter is to request the state to stop diverting or sweeping of 9-1-1 funds. Copies of such letters will be provided to the Chair of the Senate Commerce Committee, and the Chair of the House Energy and Commerce Committee, to whom the Net 9-1-1 Act Reports are submitted.

Impact on Federal Funding: The state authorities will be put on notice that if such diversions or "sweeps" occur repeatedly (say twice for States with a biennial budget cycle), there will be consequences from the federal government. One potential consequence could be a loss of federal funding for certain projects, such as highway or other transportation infrastructure projects under the control of US DOT, located in that state either on a dollar-for-dollar basis, or some type of proportional reduction.

Response: A reasonable period, 90 days or more, should be provided to a state to provide a response, although the response cannot be federally required.

The Task Force believes that the federal agencies should work cooperatively with the states, counties, and localities regarding a federal grant program administered by NHTSA, consulting with the LSAG and considering other programs at the state and local level. Many activities are already established and ongoing, which should be enhanced and continued. However, transparency is an essential part of proper governance, especially for the collection and expenditures of 9-1-1 fees. Such an early warning mechanism should serve the purpose of bringing greater transparency to alleged or demonstrated state diversions of 9-1-1 fees.

6.6 Effective State and Regional Coordination

A strong and integrated statewide and regional planning and coordination mechanism is essential for the successful deployment of NG9-1-1 systems. Some states have established, either by statute or by rule, a cohesive state coordinating body, usually within an emergency management or communications department or office of information technologies, to coordinate

the requirements, architecture, and build-out of NG9-1-1 systems. States that have a cohesive State 9-1-1 Administrator function have usually been vested with the authority to develop budgets and administer expenditures to the PSAP's, usually with some type of consultative or advisory committee with the PSAPs and 9-1-1 authorities as key stakeholders. Other states have developed effective statewide planning and coordination mechanisms involving key 9-1-1 stakeholders throughout their state.

But, quite a number of states have established neither an effective statewide 9-1-1 planning authority, nor cohesive regional planning authorities for key metropolitan areas. This is not an acceptable paradigm to accelerate the deployment of NG9-1-1 systems across the country. While there is no one-size-fits-all model, it is clear that state, regional, and local authorities need to pay close attention to these issues and develop mechanisms to increase such coordination. In particular, such authorities need to be focused intently on some of the following processes and outcomes:

- *Long-term planning that support NG9-1-1 deployments;*
- *Establishing minimum standards for such systems for the entire state;*
- *Developing the optimal architecture for the state, based on ESInet concepts developed to date, and the recommendations reflected in Section 5;*
- *Using the concept of shared services among the primary and secondary PSAPs in the state, to the extent possible;*
- *Developing consistent programs for workforce development and training throughout the state; and*
- *Ensuring that PSAP's and regional bodies develop the appropriate governance and budget accountability mechanisms within each state/regional 9-1-1 Authority.*

The TFOPA discussed various state institutional models that, while not entirely similar, appear to achieve most of the objectives outlined above. Several state models are listed below as examples of alternate approaches to achieve common goals:

Minnesota: This state has a strong regional body, the Metropolitan Emergency Services Board (MESB), to oversee the 9-1-1 system, public safety radio system, and EMS in the metropolitan area of Minneapolis-St. Paul. The Board consists of commissioners from the counties of Anoka, Carver, Chisago, Dakota, Hennepin, Isanti, Ramsey, Scott, Washington, and a council member from the city of Minneapolis. Over the years, the MESB has consistently achieved its objectives and worked cooperatively with other PSAPs and state agencies. In addition, the Statewide Emergency Communications Board (SECB) oversees issues related to 9-1-1 services, radio communication systems, and other public safety issues on a statewide basis. The SECB has a NG9-1-1 Committee which has overseen the development of a statewide plan for NG9-1-1 deployment, standards, and the build-out throughout the state. Together with other PSAPs located in less densely populated areas of Minnesota, the SECB has been able to work together with the relevant agencies to carry out these functions for NG9-1-1 in a collaborative way.

North Dakota: This state has taken a different approach by negotiating a Joint Powers Agreement with the North Dakota Association of Counties (NDACo), which carries out the statewide planning and coordination of NG9-1-1. The North Dakota Legislature established a statewide coordinating committee for this goal of statewide NG9-1-1 deployment, called the Emergency Services Communications Coordinating Committee (ESCCC). This Committee is also charged with recommending changes to the operating

standards for emergency services communications, and developing guidelines regarding the allowable uses of the fee revenue collected for 9-1-1 systems. Based on these guidelines, NDACo is responsible for carrying out these approved guidelines and plans, and achieving a timely deployment of NG9-1-1. NDACo has an NG9-1-1 Program Manager on staff to coordinate with the ESCCC and other stakeholders in the state. This entity has previously successfully managed the implementation of Phase II wireless service throughout the state, and states that it will use a similar planning model for the building out of NG9-1-1 equipment and services throughout the state.

Texas: This large and diverse state has developed a three-pronged approach to institutions governing the operations and maintenance of 9-1-1 systems, and the deployment of NG9-1-1 architecture in Texas. First, there are 25 Emergency Communication Districts (ECDs) operating under Chapter 772 of the Texas Health and Safety Code. These operate largely in large, metropolitan areas and serve 62% of the state's population. Second, there are 27 Home-Rule-City-based Municipal Emergency Communication Districts (MECDs) managed as part of ongoing city services. Third, there are 23 Regional Planning Commissions (RPCs) that operate within the Commission on State Emergency Communications (CSEC) pursuant to Chapter 771 of the Code, outside of the areas of the previous two groups and largely in rural areas. The three groups of 9-1-1 authorities have a long history of working collaboratively through mechanisms like the Texas 9-1-1 Alliance, the Municipal Emergency Communication Districts Association, and the Texas Commission on State Emergency Communications.

Alabama: Alabama 9-1-1 planning and implementation is achieved through a hybrid model of state and local government authorities. Legislative structured, 9-1-1 funding is shared between the local 9-1-1 Emergency Communication Districts (ECDs) and the state 9-1-1 Program Office. While the statewide office plays a valuable role in advancing 9-1-1 and NG9-1-1 in the state, the local ECDs carry a large role on the planning and implementation of 9-1-1 systems. On October 1, 2013, the fee structure in Alabama was modified by legislation to provide a single, monthly statewide fee on each active voice communication service connection that is technically capable of accessing a PSAP (prior to this, the fees were collected locally by the ECDs from fees assessed to wireline subscribers only, at a rate voted on by citizens in the county, complemented by a $0.70 per connection fee according to a distribution formula based on population). Currently, the statewide fee is set at a flat rate of $1.75 per connection monthly, and is collected by the State 9-1-1 Program Office. Then this Office disperses such collected revenues to the eighty-eight (88) existing ECDs, based on a designated amount.

As new funding mechanisms are developed to fund both existing systems and NG9-1-1 deployments, the TFOPA believes, as general matters, policymakers should continue to adhere to the historical construct to maintain operational decision-making at the local level, and to avoid one-size-fits-all solutions. Certain operational efficiencies are certainly possible with greater scale and scope, and the concept of shared services among the PSAPs for cybersecurity and other functions certainly makes sense (see the discussion on shared services in Section 5). Yet it is worth offering some additional context as to why state and local control of 9-1-1 systems is critical.

The PSAP operations, including calltaking and dispatch, are integrated into the operations of the first responder agencies they dispatch. The business rules of the PSAP and first responder agencies must be consistent and integrated. The PSAP call-takers must be familiar with the area they dispatch, to assist in locating callers, and to better appreciate the

circumstances of the emergency call concerns. Familiarity with specific locations and individuals, which are the source or cause of frequent 9-1-1 calls, allows the dispatcher to better determine the appropriate response, prepare first responders for the incident to which they are responding, and assist first responders.

Local officials are in the best position to appreciate the unique characteristics of their jurisdictions and agencies, and develop appropriate business rules and operational practices and procedures for first responder agencies and PSAPs. Responsibility for development of business and operational rules and operational decisions is best left with local officials with the best understanding and appreciation of the local factors impacting these policies, rules, practices and decisions.

6.7 Concerns over Dual System Funding in Transition

The TFOPA notes and agrees with the concerns raised in the recent iCERT Report about the likely lack of funding both to provide new capital for NG9-1-1 deployment while simultaneously funding legacy operational costs during the transition. Specifically, the issue of concern is that PSAP's will have to pay the current ongoing operational and support costs associated with the existing legacy system, as well as fund the additional capital and operating costs incurred for the deployment of the new NG9-1-1 solution until a complete cutover to the NG9-1-1 solution is achieved and the legacy solution is de-commissioned. In effect, as NENA and other groups have previously stated, the transition period between legacy and NG9-1-1 represents a period of increased, not lower, funding requirements. Indeed, the cost savings expected from the rollout of NG9-1-1 will only be obtained by 9-1-1 planning agencies that have the ability to sustain the "double costs" of the transition era until the legacy system is de-commissioned and only NG technologies remain in use. The longer the transition timeframe is for a PSAP, the greater the costs will be that will be incurred as a result of this necessary and inevitable overlap of the costs of the two systems. The dual, and sometimes duplicative costs, will constrain the rollout of NG9-1-1, and in some cases, have a potentially terminal impact on jurisdictions that simply don't have the funds to pay for two systems. Lack of adequate 9-1-1 funding to sustain the migration from legacy to NG9-1-1 will slow the overall transition time to fully functioning NG9-1-1 technologies.

While a sound transition plan to NG9-1-1 does in fact require a methodical migration strategy, State and federal policy officials can play a critical role with expediting these plans by encouraging and facilitating a sound and methodical migration strategy. In this report, the Task Force sets forth both the overall policy principles as well as principles for more effective state and local coordination on such strategies. In addition, the Task Force suggests that Congress may wish to consider providing certain sources of federal funding to accelerate such a transition. While the Task Force has not reached consensus, the general belief is that the policymakers at all levels need to engage seriously in a targeted discussion about a date by which nationwide adoption of NG9-1-1 will be achieved. More specifically, although the TFOPA realizes that it is not legally enforceable, it does recommend to the state and local governments that they reach a consensus soon on a targeted date, for example 2024, by which national deployment of NG9-1-1 would be completed. Such an objective would assume some sort of targeted federal grant program, with conditions, cited above, reducing or eliminating the number of states that divert 9-1-1 fees for other purposes, and other recommendations in this report. In short, such a policy would target not only a date as a national objective, but also would be a collaborative and coordinated effort from the ground up with local and state governments.

One example may help illustrate both the complexity and importance of this need to shorten the transition period. One area where the problematic nature of the dual costs can be seen is with respect to the existing connections to the legacy Selective Router(s) serving a PSAP service area. During the transition to NG9-1-1, PSAP's will likely incur both the ongoing cost of current connectivity to the Selective Router(s) supporting the legacy 9-1-1 service, while at the same time paying the IP connectivity costs for the NG9-1-1 solution that is being deployed. Actual duality and magnitude of the Selective Router costs will vary depending on what the policy and regulatory framework is within each state, and by the 9-1-1 service providers billing policies. However, the opportunity for potentially onerous, "double billing" is clearly seen in this one example. Without proper resources, 9-1-1 planning entities needing to advance its public safety systems will be left paralyzed.

6.8 Possible Funding Alternatives

The TFOPA believes that greater efforts must be made to consider alternative funding models to quicken the transition to NG9-1-1. For decades 9-1-1 has been dependent on fees placed first on landline telephone subscriber bills, then with fees on post-paid wireless subscribers, and then in most states, fees on pre-paid wireless subscribers at the retail level. As more consumers cut the wireline "cord," moving to wireless-only households, 9-1-1 fees have in some cases dropped significantly. Still, there are states that do not have a pre-paid wireless 9-1-1 fees.

The TFOPA had a very short time schedule in which to examine the funding alternatives, develop its analysis, and make its recommendation. It was not possible to integrate this work on funding alternatives more holistically with the results of Sections 4 and 5, although that will be possible later. It was not possible to run detailed case studies or scenarios, with certain assumptions for architecture and security, and discuss the preferred funding scenario for those cases. Instead, the TFOPA chose to focus on the highest priority issues in funding today, both the gaps and the prospects going forward in an all-IP network system, and to develop recommendations at a high level.

Moreover, as stated earlier in the Executive Summary, the TFOPA stresses that this a menu of options for all policymakers at the state and local government levels to consider, as well as federal agencies and others in the 9-1-1 ecosystem. This is not meant to be a requirement at either the federal, state, or local level, and TFOPA is not recommending adoption of one option over another. Instead, the TFOPA urges serious consideration of these proposals, and the analyses that led to the recommendations. Many details and adjustments remain to be discussed and resolved, if such mechanisms are to be adopted by state and local governments. As stated earlier, no system will be perfect, adjustments will have to be made, and transitions by nature are always somewhat complex and messy. The joint advisory committee, or LSAG, will be asked, at a minimum, to take up some of these detailed issues and discuss them. Another alternative would be for the TFOPA itself to examine these issues in more granular detail over the remaining time of the TFOPA. That is a decision for the FCC. What follows is the discussion of approaches that the Task Force believes deserve serious consideration as priorities for funding mechanisms that may alleviate some of the stresses of the current funding while being consistent with the policy principles.

6.8.1 Network Connection Fee Approach:

6.8.1.1 Background:

The TFOPA recommends the consideration of a transition to a "network connection fee" which would assess 9-1-1 fees on end user connections to the facilities-based communications providers over whose facilities voice telephony and other communications with a PSAP can be initiated. The intent is to treat equally all facilities-based network connection providers on whom 9-1-1 fee collection and remittance can be practically enforced. Also, such a fee would treat equally providers of non-facilities-based communications capabilities provided over those network connections (including capabilities provided by the facilities-based providers) on which no fee would be assessed. This recognizes the developing distinction between the interdependent markets for network connections (to the PSTN and the Internet), and for voice telephony and other outgoing or upstream communication capabilities over bandwidth.

IP-enabled broadband and Wireless IP-enabled data services ("IP-enabled services") are supplied by providers who have invested in physical plant within a state and local jurisdiction necessary to supply the service, whether twisted pair, coaxial cable, fiber, or the interconnected towers and antennas of a wireless system. These IP-enabled services provide a connection to the public Internet, and through gateways to the PSTN, which can be used by independently provided telephony and other communications services. That is, VoIP service can be provided by the IP-enabled services provider ("Facilities-based Provider) or by third parties with no physical facilities in the state or the country ("Non-Facilities-based VoIP Provider"). The Facilities-based Provider is readily identifiable and its 9-1-1 fee obligations on its VoIP service offerings are practically enforceable by virtue of its having physical facilities in the jurisdiction, while it is more difficult to even identify Non-Facilities-based VoIP Providers that lack any facilities within the jurisdiction. The VoIP customer base is also spread among a larger number of providers, increasing the costs of enforcing 9-1-1 fee obligations even if the VoIP providers can be identified. It is not a surprise, then, that the public safety community reports that 9-1-1 fees appear to be reliably remitted by facilities-based providers, while Non-Facilities-based VoIP Providers supplying service in some jurisdictions are often not even known.[88]

Today, 9-1-1 fees are established to provide the revenue required for a 9-1-1 Authority to meet the costs of providing 9-1-1 service, or some defined subset of those costs. If some end users of communications services subject to the 9-1-1 fee are not paying a 9-1-1 fee, either because they subscribe from a Non-Facilities based VoIP provider or purchase prepaid minutes from vendors which do not collect and remit the 9-1-1 fee, then other consumers paying the 9-1-1 fee must bear the resulting shortfall in the 9-1-1 Authority's revenue requirement. In a sense, this is a classic free rider problem in which certain market participants have the ability to benefit from the public good of ubiquitous emergency communications systems for society at large, but not pay an equitable share of the costs.

Independent VoIP providers and Independent Retailers not collecting and remitting 9-1-1 fees typically enjoy a price advantage in marketing their services compared to facilities-based VoIP providers since those providers reliably collect and remit 9-1-1 fees. Rational end users will respond to this price advantage by taking service from the Independent VoIP Providers and Independent Retailers, decreasing the pool of users across which the cost of 9-1-1 service can be spread, and increasing the amount of 9-1-1 fees which must be assessed on the facilities-based

[88] Gateway providers can identify VoIP providers terminating traffic within a jurisdiction, but cannot necessarily identify VoIP providers with traffic originating within a jurisdiction.

VoIP providers and prepaid service providers. 9-1-1 fee reforms must be implemented in response to the changing structure of telecommunications services and markets, to make these programs sustainable.

6.8.1.2 Foundation for an equitable 9-1-1 fee on IP services:

As consideration is given to transitioning to a network connection fee model for IP-enabled services, the following three factors should be evaluated as to their ability to ensure one of the key policy principles – sustainability:

a. The vast majority of communications services that can be used to contact a PSAP continue to require a network connection located within the state and/or local jurisdiction.[89] Assessment on the network connection over which an emergency call could be placed, should be able to collect equitable 9-1-1 fees being collected from every end user of a communications service on similar terms and conditions.

b. The reliable remittance of 9-1-1 fees on VoIP services supplied by facilities-based providers but not by some non-facilities based VoIP providers creates a situation in which the terms of market competition are not equal. Non-facilities Based VoIP Providers could potentially, create the inequitable scenario discussed above, by not collecting and remitting 9-1-1 fees for Public Safety. Further analysis is required to determine if this competitive disparity can be addressed by having facilities-based providers assess fees on over-the-top VoIP providers, and as a result, whether imposition of 9-1-1 fees on the network connection over which VoIP or other communications services are provided would create more equal, competitively neutral market conditions for facilities-based providers of VoIP and other facilities-based services. Under this revised approach, the intent would be to ensure that no provider of VoIP or other voice or data services provisioned over the same network connection would be subject to an additional 9-1-1 fee.

c. This proposed network connection fee might also promote the implementation of comparable terms and conditions for all users through their network service providers, including traditional wireline, wireless and broadband service providers, regarding how they assess and collect E9-1-1 fees on those end-users. In order to prevent inequity and duplication in fee collection, wholesale voice and data services (voice and/or data services for which no end user connection exists) would be excluded. The TFOPA believes that such a framework would support the principle of technological and competitive neutrality, cited above. Each competing network connection (network access) provider would collect and remit 9-1-1 fees for connections over which their customers can originate communications to a PSAP. Ideally, no facilities-based provider would enjoy a price advantage by virtue of application or enforcement of 9-1-1 fees because all providers of physical connections to the PSTN or public Internet would be responsible for collection and remittance such fees to the relevant 9-1-1 Authority, which would be an enforceable obligation pursuant to state law.

There is a substantially smaller number of facilities-based network-connection providers and potential broadband service providers, compared to over-the-top VoIP and other service

[89] Satellite-delivered services that might be used to contact a PSAP require specialized equipment, are expensive, require a service agreement and have relatively small number of users, and as a result may permit effective implementation of a fee program.

providers. This is a result of the vast difference in the investment required to deploy a telecommunications network as compared to the cost of developing and providing non-facilities based VoIP applications and/or services. The TFOPA also anticipates a continuing trend of VoIP and other communications functionalities being incorporated in cross-platform applications, including gaming, productivity and social media applications, and even of new operating systems for traditional computing devices. Such integrated cross-platform applications not only increase cross-functional utility but also enhance tracking of user information permitting developing of additional revenue streams from highly targeted advertising. As such business models continue to evolve dynamically over time, the TFOPA believes that a network connection fee on services that allow communication to Public Safety from end users will be more effective both from a revenue collection and auditing standpoint due to the smaller number of entities assessed. Finally, questions may arise regarding the legal aspects of the imposition of such a fee for 9-1-1 purposes given the likely continuation of the Internet Tax Freedom Act (ITFA), whose continuance is now pending in Congress. Working Group 3 members discussed this issue, and the majority believe that these recommendations appear to be consistent with the safe harbor provisions for 9-1-1 and E9-1-1 services in the Act. However, some disagreed and a more comprehensive legal analysis may be necessary. Moreover, Congress may wish to clarify its intent regarding the interpretation of the ITFA as NG911 systems are implemented further.

6.8.2 Potential Components of a Network Connection Fee

In most or all states, legislation will be required to implement a network connection fee. Public safety entities and service providers should participate in the development of the legislation to ensure that such a fee mechanism meet the policy principles enunciated above, especially that of technologically and competitively neutral (or equal treatment for equal services). Set forth herein are some issues for consideration at a high level, which will need to be discussed in more detail by the LSAG or another body. Additional refinements of a network connection fee program appropriate to an individual state will likely be necessary.

With wireline and wireless service, users pay a separate and additional 9-1-1 fee on each line of service. Business users currently pay a fee based on the number of lines derived from a telephone trunk into their phone systems. To be equitable, a network connection fee on end user broadband services. However, the relatively small amount of bandwidth required to place a voice call over a broadband connection requires that any capacity-based fee be carefully designed to be equitable to broadband VoIP users.

The overall construct for such a fee collection system can be broken down as follows. A 9-1-1 fee would be collected and remitted by local exchange carriers on each active access line connection over which an end user could currently initiate a call to 9-1-1. A line over which DSL service was being provided would not be deemed an access line connection, and would be assessed a 911 fee as a broadband service, as discussed below. In the context of a residence or a business with multiple active access lines, a fee would be collected for each active access line, pursuant to state law and rules

The CMRS services are personal communications services, with each account user having a separate device and, in many states, being charged by the CMRS provider for wireless access for each device. If a family or business account has multiple users and devices, the the CMRS provider assesses a charge for each device on either a monthly basis for postpaid services, or at the point of sale (POS) for prepaid services in the thirty-seven (37) states where

authorized. This is consistent with current practice. Under existing 9-1-1 fee programs in many states, a separate 9-1-1 fee is assessed on each CMRS device, and not separately for (i) CMRS voice access and (ii) wireless data plan (broadband) access over which VoIP calls might be made, using the same device.

Under a connection-based fee program, a single surcharge per account-user device would continue to apply. In the event a CMRS provider were to introduce a service featuring a high-bandwidth broadband service to a wireless access point for use by multiple devices, a single surcharge per account-user device would apply whether the user subscribes to voice, data, or both services, but would apply to the network connection rather than the voice or other service the CMRS supplies using the network connection. The fee would be assessed on some defined unit of network connectivity. However, it would be duplicative for a state to charge a fee on both a per device basis, and a connection fee basis for a broadband connection serving multiple CMRS devices should such services be offered in the future.

Consistent with principles outlined in this report, there also should be no duplicative assessments for facilities-based VoIP providers over which end users can connect to a PSAP. Such assessments should either be based on the end user's ability to access 9-1-1 services, e.g. based on traditional access line basis for POTS, or on a network connection fee for broadband services using facilities-based VoIP. In all cases, regardless of the assessment methodology chosen, the broadband services provider should be responsible for assessing, collecting, and remitting to the 9-1-1 Authority the full amount of the 9-1-1 fees. This would continue the traditional practice, consistent with the principles of cost causation, which the beneficiaries of the 911 services – namely the customer or end-user – should ultimately pay for the NG9-1-1 transition and the ongoing operations of 9-1-1 systems. Moreover, since the TFOPA believes that the dedicated 9-1-1 fee approach should be continued, broadband service providers that provide the capability for communication to PSAPs should be responsible for the collection and remittance of such fees to the State 9-1-1 Authority as they move through the NG9-1-1 transition.

The advantages of moving to NG9-1-1 using broadband services include the ability to enable transmission of photos, videos, and other data-rich transmissions from the customer to the PSAP. However, broadband services are not provided by "access lines", each of which can be used to establish a single channel of voice communication. Instead, such service is provided in bandwidths permitting many more voice channels to be derived than may actually be used by the customer. These complexities and challenges will have to be resolved in more detail by this Task Force in its next phase or by the LSAG in further deliberations. The challenge posed by broadband service for 9-1-1 fee assessment is that for a residential consumer it provides bandwidth many times that available with dial-up access or for a single VoIP connection. However, in a business context, a broadband service may serve an IP-PBX at the business customer premises.

The TFOPA believes that further deliberations on the details of an end user network connection fee associated with end user services should be further studied. There are a range of options to determine the appropriate usage-based fees under such an approach and further study should address the options.

In summary, the Task Force believes that an end user network connection fee on subscriber service that allows communication to Public Safety services warrants further consideration as a 9-1-1 funding option for the future. The TFOPA realizes that only a high level analysis of such a fee methodology has been provided, and that much work remains to be

done to deliberate over the complexities and details of this approach. There may be other methods for 9-1-1 fee collection assessed on end users of broadband services through their providers in a clear and equitable manner, but such methods were not consider as any specific alternatives in the short timeframe given for the current report. The TFOPA recommends that either the LSAG, described below, or the next phase of this Task Force address such issues in detail.

6.8.3 Potential path forward for prepaid wireless plans

6.8.3.1 Background

For prepaid wireless service plan sold at POS, the unity between the service provider and the billing and collections provider has been severed. That is, a customer pays in advance for a quantity of minutes of voice communications/text messages to use on the customer's wireless device, separate from purchase of the device. The quantities of minutes can be purchased from the prepaid service provider, or from any of thousands of Internet and brick and mortar retailers ("Independent Retailers"). In the vast majority of states in which 9-1-1 fees are assessed on prepaid service, the 9-1-1 fees are required to be collected at the POS through the retailer, submitting to the State Department of Revenue.

Similar to VoIP service discussed above, the 9-1-1 community reports that it appears the wireless service providers and large retailers reliably collect and remit POS 9-1-1 fees. With that portion of prepaid minutes sold by thousands of smaller retailers and Internet retailers spread across the number of outlets involved, the cost of enforcing collection from any individual retail outlet will often exceed the benefit, and enforcement may also be impractical for Internet vendors located outside a jurisdiction. The 9-1-1 Community reports that annual 9-1-1 fees paid by users of prepaid wireless services do not equal those paid by users of postpaid services, and that prepaid surcharge 9-1-1 fees fall far short of the amount which should be received given the quantity of prepaid minutes sold and used. Collection authorities may not even know which independent retail outlets sell prepaid minutes to "recharge" prepaid services.[90] On the other hand, the wireless industry alleges that some of this variance can be attributed to the non-monthly purchasing pattern for prepaid users, juxtaposed with the by-month revenue requirements and planning requirements required by 9-1-1 Authorities.

6.8.3.2 Short-term solution

As with wireless service in general, transition to a network connection-based 9-1-1 fee program will have little impact on collection and remittance of prepaid wireless services, at least in the short term. A surcharge will continue to be assessed on the purchase of prepaid minutes enabling a user to connect to and use the wireless network.

The difficulty presented by prepaid wireless with collection and remittance of 9-1-1 fees is the large number of Independent Retailers (retail outlets which are not owned and operated by the prepaid service providers) which sell prepaid minutes, and the fact that the incremental 9-1-1 fees which should be collected and remitted by each of these entities frequently makes enforcement uneconomic. The sales of prepaid minutes by Independent Retailers that do not

[90] Some states establish the amount of 9-1-1 fees on prepaid service with the intent of producing the same total annual 9-1-1 fees for the average prepaid service account as for postpaid service. Other states establish the 9-1-1 fee on prepaid service to produce the same relative fee as compared with the amount of the 9-1-1 fee assessed on the average monthly use and charge for postpaid service.

collect 9-1-1 fees, may undercut sales of prepaid minutes by Prepaid Service Providers. The wholesale prices of prepaid minutes necessarily includes a profit margin for the Prepaid Service Providers, and the wide availability of prepaid minutes through such Independent Retailers may be more important to the prepaid business model than the additional margin. Prepaid Service Providers do not have knowledge as to which, if any, of their wholesale Independent Retail customers do not collect or remit 9-1-1 surcharges, and therefore, do not have the ability to or economic incentive to discipline bad acting Independent Retailers. In addition, state collection authorities have no independent knowledge of, or audit capability of, the Independent Retailers selling prepaid minutes, nor the volumes of their sales.

The POS 9-1-1 fee system has been established in thirty-seven (37) states. Therefore, in the short-term, the TFOPA urges the remaining states to enact legislation as quickly as possible in order to enable the collection of adequate 9-1-1 fees from pre-paid plans. A POS 9-1-1 fee system has been considered necessary because of the difficulty of collection and remittance of prepaid surcharges by the Prepaid Service Provider at the wholesale level when each state may establish a different surcharge amount and distribution methodology.

6.8.3.3 Longer-term solutions

The development and implementation of a more effective, reliable and equitable fee collection system for prepaid service would appear to require collaboration and coordination among the states. At a minimum, the additional information cited above from both prepaid service providers and collection authorities would provide a foundation for such coordination. Such longer-term coordination and collaboration, and the sharing of confidential information subject to non-disclosure provisions, will require additional time and efforts. The TFOPA simply did not have sufficient time, resources, and capabilities to collect such information with the appropriate safeguards and analyze it properly in the context of this Report. Therefore, it is recommended the joint advisory committee, or LSAG, take up these issues in a timely way and examine both the data and arguments for this issue, and make recommendations to the 9-1-1 authorities at the state and local level.

6.8.3.4 Alleged under-recovery of Pre-paid Wireless Plan Fees

The Task Force has received credible evidence suggesting an under-recovery of 9-1-1 fees through the prepaid wireless plan providers.[91] Nationally, such under-recovery is alleged to be in the amount of $276 million across the states that have prepaid wireless 9-1-1 fees, compared to what would be expected in 9-1-1 fee revenues under traditional post-paid wireless subscriptions where the 9-1-1 fee is listed as a line item on the consumer's bill. However, the Task Force has also been advised that the wireless industry has not been able to thoroughly vet this study, including its underlying assumptions and sources of data. Accordingly, the Task Force believes that these issues should be taken up immediately by a joint advisory committee, or LSAG.

Moreover, members of the Task Force expressed concerns over the amount of administrative fees collected both by the state departments of revenue and by the independent retailers who collect this fee at point-of-sale. Some members of the Task Force expressed concern that the POS 9-1-1 fee for pre-paid wireless plans is being collected inconsistently and is not uniform across all carriers. The Task Force believes that such analyses are legitimate and

[91] "Prepaid-Still Short-Changing 9-1-1" working paper, author Joseph Barrows, State 9-1-1 Coordinator and Executive Director of SMRS Board, State of Kentucky, September 2015.

need to be taken seriously in order for adequate fees to be remitted to PSAPs throughout the country on a comparable basis as post-paid wireless plan subscribers. Some carriers allege that this under-recovery may primarily be attributable to the failure to accurately forecast for the variance in purchasing patterns between pre-paid and post-paid communications by wireless customers. However, due the brevity of deliberations and the lack of adequate time to verify these allegations, the Task Force believes it is more appropriate to refer these issues for timely and detailed examination by the Local State Government Advisory Committee recommended below.

6.9 Education and Outreach

The 9-1-1 community needs to adopt a more systematic and disciplined way of reaching out to the decision-makers and policymakers that decide the public policies and specifically the state budgets around the country. As stated throughout this Report, this recommendation should be viewed within the complex environment of state laws, practices, and the budget-making policies in each of the state Legislatures and Governors' Offices. Overly simplistic solutions and approaches should be avoided. At the same time, the Task Force believes that this is an urgent time to engage in a more active dialogue on these issues, and correct some of these practices to accelerate the deployment of NG9-1-1 systems.

The creation of a Local State Government Advisory Committee on 9-1-1, described below, is an important element of such an effort. To create a sustainable, technology-neutral fee structure, a sustained organizational effort between the FCC and federal agencies, states, and PSAPs must be encouraged. In addition, ensuring that accurate information on state and local budget practices is collected, audited, and analyzed in the proper way is another vital part of this effort. Transparency of information, of course, is an essential part of good governance at any level. The Task Force has concluded, however, that putting this principle in to practice in such a complex area across multiple jurisdictions requires more efforts, including the possible use of outside auditors to confirm the accuracy of such data and information before its submittal to Congress.

The key actors in this education and outreach effort will be the governmental agencies involved in managing and overseeing the 9-1-1 system, namely the FCC (specifically the PSHSB), members of NENA, NASNA, NARUC, and APCO. These constitute the three layers of governmental jurisdiction over the national 9-1-1 system, and recognize both the inherently local nature of 9-1-1 call taking and dispatching while at the same time understanding the benefits of more uniform NG9-1-1 system architectures and technology. Each of the trade associations is a members-oriented organization with policies and priorities driven from the bottom up through its membership. Therefore, such organizations are the optimal means for an enhanced outreach and education effort.

Key leaders and organizations should be identified to help educate and inform policy makers at all levels of government about the need for NG9-1-1 and the benefits it provides their constituents. The goal is to enable these organizations to step forward and address issues, such as funding, associated with deploying NG9-1-1. Some states prohibit state and local government employees from lobbying their state officials, while others do not have such restrictions. Time and resources are not overly abundant, and must be husbanded and targeted carefully toward key decision-makers. A key group of such leaders should be identified for educational efforts about NG9-1-1 and its funding. The perceptions and views among Legislators, for example, may not change overnight since many of the state policies and practices have been in place for some time. Nonetheless, many existing funding models are

proving to be insufficient due, in part, to the advances in technologies. Thus, policy makers responsible for 9-1-1 should be the best informed about the needs associated with the deployment of NG9-1-1.

Each of the associations involved in 9-1-1 issues – NASNA, NARUC, NENA and APCO and others – have several regular meetings throughout the year. These are ideal venues where 9-1-1 issues are discussed and debated. These discussions are already occurring within these organizations and awareness is being raised on the 9-1-1 fee and resource allocation issues, as evidenced by the 2015 summer meeting of NARUC in New York City, and the summer meeting of NENA and related meeting of NASNA in Denver. While these discussions are important within the "9-1-1 ecosystem", more efforts need to be targeted on associations and thought leaders outside of this ecosystem.

Such an education and outreach efforts needs to be focused on some of the following associations and groups:

Governors: There are various organizations representing the Office of Governors, but the TFOPA believes the best place to start is the National Governors Association's Center for Best Practices. It has been active in cybersecurity policies of the states recently, highlighting the importance of state fusion centers, and therefore, the overall report of the TFOPA should be of interest. This education and outreach effort must be a non-partisan effort, but it would also be useful to reach out to the Democratic and Republican Governors Associations as well, since they also hold meetings each year. In addition, the regional meetings of the Governors should be considered as appropriate venues to engage in a dialogue on these issues.

Legislatures: Again, there are various groups that represent legislative bodies throughout the country, and the meetings of these associations should also be considered for targeted outreach activities on NG9-1-1. As stated earlier, the National Conference of State Legislatures (NCSL) has followed the 9-1-1 and Enhanced 9-1-1 activities and legislation across the states for several years, and therefore would have an interest in hearing about the analysis and recommendations in this Report. The Council of State Governments (CSG) also should be considered since both it, and its regional affiliates, hold meetings several times a year, and have an interest in technology and homeland security/public safety policies. Finally, again recognizing that this effort should be non-partisan, this key leadership group should reach out to the American Legislative Exchange Council (ALEC) as well, since they have a Task Force on Communications and Technology that has followed these policies for several years, and organizes a large annual meeting and other conferences throughout the year.

In addition, state Chief Information Officers (CIO's) and the state Attorneys-General should be included in the education and outreach activities, since they do play an important role in communications and technology policies in the state. They are represented nationally by the trade associations of the National Association of State CIOs (NASCIO), and the National Association of Attorneys General (NAAG) which are represented with offices in Washington, D.C. and can be contacted. Finally, in the interests of consumers, the residential and small commercial users of communications services, should not be neglected in these activities, which are represented nationally by the National Association of State Utility Consumer Advocates (NASUCA).

In addition to the focus on the above national associations, education and outreach activities should focus on certain states and regions. While a single-minded focus on the "diversion states" is misplaced and that the budgetary issues are much more complex, the leadership group for outreach needs to engage with the states listed in the most recent Net 9-1-1

Report who have reallocated 9-1-1 fees for non-9-1-1 specific purposes. If there were a Local State Government Advisory Committee on 9-1-1, then hopefully it could lay the groundwork for such a dialogue in those states. Another priority group of states for such a dialogue would be those with limited or no statewide or regional 9-1-1 planning or coordination authority, as described above. Such a statewide body is a critical element in ensuring a comprehensive build-out of NG9-1-1 systems. There are a number of "hybrid" states, a number of states with authority over wireless services only, and also a number of states where most of the authorities for planning and deployment rest with the PSAPs at the county level. In some states, the statewide 9-1-1 Authority has little authority over the fee mechanism, the expenditures, and the planning for NG9-1-1. Again, the emphasis here should be on establishing the grounds for a constructive dialogue about the unique needs of NG9-1-1 architecture and deployment, the need for sustained long-term planning at a statewide level, and the other factors mentioned above. A partnership is required between the state and county if this is to be a successful effort, especially given that new legislation will undoubtedly be required in order to adopt the network connection fee mechanism and other recommendations in this Report. Unity of effort will be critical to passing such legislation.

6.10. Local State Government Advisory Committee (LSAG) on 9-1-1

Finally, the Task Force, as mentioned previously, believes that the creation of a federal, Local State Advisory Committee on 9-1-1 (LSAG) is essential to carrying out some of the recommendations in this Report. In fact, the creation of such a joint consultative mechanism by the Commission is long overdue. This Report marks a call for action for both the 9-1-1 community and for the larger group of decision-makers and policymakers in the states and counties around the country. To create an environment for sustained long-term planning and deal with the complexities of fee mechanisms and governance structures, an advisory committee is a useful vehicle to encourage more visibility to these issues. The TFOPA also urges the Commission to make such an advisory committee permanent, in order to allow a core group of 9-1-1 experts to deliberate; if not permanent, allow Members to be appointed from a diverse group of 9-1-1 experts throughout the country on a rolling, multiple-year basis.

While the Task Force has not discussed the membership and mechanics of such an advisory committee in detail, the TFOPS offers the following suggestions for the Committee, which would operate under the auspices of the FCC, and be subject to Federal Advisory Committee Rules, or FACA. The committee should be composed of a relatively small group of representatives of government agencies involved in 9-1-1 issues such as NASNA, NARUC, the FCC, county organizations and other state organizations. There should be a contributing role for other participants in the "9-1-1 ecosystem", which should include representatives from NENA, APCO, iCERT, 9-1-1 experts from trade and industry associations, a range of equipment vendors, service and data base providers, and other groups associated with NG9-1-1 architecture and deployment. In a general sense, such as a LSAG would be quite similar to the current structure and membership of the TFOPA, but would seek its primary membership from governmental officials involved in 9-1-1 at the local, state, and federal levels.

A first order of business for the 9-1-1 LSAG could be to oversee the quality of data and analysis submitted by the states for the Net 9-1-1 Report to be submitted to Congress. Some external review of this information would help ensure the information is correct and reported accurately. Another priority item for discussion would be the structure of the pre-paid wireless plan 9-1-1 fees, and assessing in more detail the allegations that such plans are significantly

"under-collecting." The advisory committee could flesh out more details of the proposed network connection fee and make recommendations on any adjustments or fine-tuning of this fee mechanism. In addition, the scope of the responsibilities of this advisory committee should not be limited solely to NG9-1-1 deployment issues, but should include other policy and funding related issues for 9-1-1 that pose common challenges to state and local governments where a federal role would be constructive.

This advisory committee, however, should not involve itself in issues related to the daily operations and maintenance of the PSAPs, including engineering issues related to PSAP architecture/ESInets, "gaps" in governance and accountability raised in the FCC's Notice of Proposed Rulemaking (FCC 14-186), and to major 9-1-1 outages and any enforcement actions or state adjudications related to specific carriers. State 9-1-1 Administrators, State Commissions, and PSAP's and county governments are established for these purposes, and procedures under existing laws and rules adequately address these issues. Instead, the focus of the advisory committee should be on higher level, policy-related issues that relate to existing fee mechanisms, ensuring the accuracy of information submitted to the FCC and to Congress, and deliberating on targeted policies and issues that are common to most state and local jurisdictions.

Such an advisory committee also could provide a regular means through which government officials could communicate in a more efficient and focused way with external stakeholders in selected States as described in the education and outreach section above. . Together with the other recommendations in this Report, the TFOPA believes this offers a comprehensive, sensible path forward to achieve our common goals of ensuring a robust emergency communications system and continuing to save the lives of many Americans.

6.11 Conclusion

The Task Force respectfully offers the forgoing as a way to stimulate a broader conversation at the Commission, and especially with the staff and leadership of the PSHSB. Ultimately, it is the Commission's decision whether to move forward with any of the other recommendations in this Report.

7 Findings and Recommendations Summary

This final report is organized around the three major PSAP focused work efforts of the TFOPA which includes Optimal Approach to Cybersecurity for PSAPs (Section 4), Optimal Approach to NG9-1-1 Architecture Implementation by PSAPs (Section 5), and Optimal Approach to Next-Generation 9-1-1 Resource Allocation for PSAPs (Section 6). Section 7, Findings and Recommendations, is a summary of all recommendations contained throughout the report and organized by the work effort.

7.1 Optimal Approach to Cybersecurity for PSAPs

This part of the report provides a set of recommendations to public safety leadership specific to Optimal Approach to Cybersecurity for PSAPs. 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. A very high level summary of these recommendations is as follows:

- The TFOPA has determined that an additional layer, identified as the Emergency Communications Cybersecurity Center (EC3), should be introduced into the recommended future architecture.
- The local PSAPs, 9-1-1 Authorities and regional organizations can leverage a number of existing capabilities, such as the DHS NCC, NCCIC, Information Sharing Analysis Centers (ISACs), Information Sharing Analysis Organizations (ISAOs) 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.
- 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.
- Public / Private Collaboration is critical to the success of a comprehensive cybersecurity approach,
- Governance is pivotal to secure and interoperable emergency communications. The TFOPA 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.
- The TFOPA 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. It is recommended 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.
- 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 Task Force recommends that PSAPs and 9-1-1 Authorities use the included chart as a baseline document for identifying training needs and planning accordingly. In addition, as the Task Force was somewhat limited on time to further study this area, additional work may be merited by future iterations of the TFOPA.
- The TFOPA has limited the 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.
- The TFOPA 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 Section 5.

- The TFOPA recommends that PSAPs and 9-1-1 Authorities conduct a logical analysis of each potential architecture option as recommended in Section 5, and then consider integration of the core cyber services, local PSAP workforce, and the ICAM recommendations, and collaborative information and data sharing as part of the overall NG9-1-1 implementation process.
- The TFOPA has developed a checklist based on previous work done by multiple organizations. 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.

It is the conclusion of the TFOPA members that further examination of the recommendations contained in this report should be considered as part of any tasking for future iterations of the TFOPA, or the TFOPA related activities. In conducting this work, the TFOPA 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.

7.2 Optimal Approach to NG9-1-1 Architecture Implementation by PSAPs

This work is not exhaustive. Additional guidance needs to be developed to best make use of this information, and the TFOPA encourages the Federal Communications Commission to charter such efforts as part of the 2016 TFOPA initiatives. Potential topics to be explored could be the potential costs of transition, comparative early developer use cases, additional study of access for people with speech and hearing disabilities, and the integration of applications that provide access to the 9-1-1 system.

The Task Force is aware that communications and communications technologies like the Internet of Things (IoT), OTT Apps, analytics, and other new networking technologies continue to rapidly evolve and will eventually become part of the public safety ecosystem. How these technologies will affect public safety and effect how emergency response is executed in the future is a topic for potential further consideration. As the public safety technology ecosystem expands, how the new technologies and capabilities will be integrated into the NG9-1-1 environment will be an important consideration for future study and analysis.

A primary message in this report is that NG9-1-1 architecture can be customized to support almost any configuration of PSAP operations. Factors that affect these configurations include financial, political, governmental and operational considerations. An overall goal of this report was to educate 9-1-1 Authorities and policy officials so they have an understanding of NG9-1-1, its components, capabilities, deployment options, and potential benefits.

Armed with this understanding, 9-1-1 Authorities and decision-makers will be able to apply that knowledge to ongoing objective and collaborative dialogues that will enable them to craft a NG9-1-1 plan that meets the needs of their jurisdictions, ensuring all citizens including persons with disabilities have direct access to 9-1-1. As stated throughout this report, it was not the intent of the Task Force to recommend a particular configuration for the deployment of NG9-1-1, therefore this report is absent a “one-size fits all” architectural recommendation. The Task Force did feel it important to identify key “Findings and Considerations” contained in this

report that 9-1-1 Authorities might consider to assist in the planning and deployment of a NG9-1-1 system. The following represents the highlights of those considerations:

POLICY/REGULATION

- Legacy terminology is not always as precise as it needs to be; and in this transformative time in the evolution of 9-1-1, terminology that applies to NG9-1-1 should be more detailed and specific.
- Providers of 9-1-1 services must be accountable for the reliability of their services, and vendor contracts, buttressed by state-sanctioned tariffs where needed, can provide an effective means to address the availability and reliability of 9-1-1 service.
- While the transition to NG9-1-1 will bring significant benefits, it must be accomplished in a manner that does not undermine the availability, reliability, and resiliency of the 9-1-1 system.
- Consistent with existing law, regulatory policies should continue to recognize the distinction between access to the 9-1-1 system provided by Originating Service Environments and their vendors, and the 9-1-1 system itself provided by 9-1-1 System Service Providers that contract with states, regions, and local authorities for provisioning of various 9-1-1 services. As the transition to NG9-1-1 occurs, considerations should be given to whether and how the distinctions between these roles will impact overall 9-1-1 reliability. Jurisdiction in certain areas of 9-1-1 access to PSAPs is yet to be defined (e.g., applications, VoIP, etc.).
- The legacy single 9-1-1 service provider environment upon which most of the current 9-1-1 regulation was formed will need to be readdressed in the current NG9-1-1 market. Regulations that addressed needs in the legacy 9-1-1 world need to be reevaluated to determine if they are still relevant and, in some cases, may create unnecessary barriers to transition to NG9-1-1.
- Since existing statutes and regulations vary widely among jurisdictions. Therefore, it will be important to assess to what extent they allow the implementation of new technologies and optimizations such as the sharing of resources and merger of PSAP operations. Any significant differences will have to be addressed before any formal action can be taken toward sharing resources.
- Effective communications and coordination among political leaders, public safety agency leadership, and the general public will be important in addressing concerns and managing expectations of all stakeholders. In this process, both legislative and regulatory arrangements at all levels of government that extend oversight into the 9-1-1 environment may require reexamination and some existing statues, policies, rules and regulation will certainly require modification in order to effectively support NG9-1-1 implementations.

GOVERNANCE

- A national system enabling the collection and analysis of standardized administrative data, operational data, cost data and CAD data should be developed and made available to PSAPs and 9-1-1 Authorities, to provide essential information to substantiate decisions and improvements.

- Further enhancements to the governance/regulation of 9-1-1 systems and services should be developed by an advisory committee comprised of organizations such as NARUC, NASNA, NENA, APCO, and other organizations representing state, local, regional 9-1-1, and industry officials, whose recommendations would be augmented by public comment.
- Public safety agencies often contract with their 9-1-1 service providers for such services as network operations center (NOC) functionality and related features. Contracts should include Service Level Agreements (SLAs) and other provisions to assure service quality and reliability, which provisions will likely need to evolve in scope going forward.
- New governance structures designed to optimize the potential benefits of NG9-1-1 must be based on mutual agreement and formalized by 9-1-1 Authorities. The form of the agreement should be based on state statutes or local ordinances and should set standards for what is considered successful performance.
- NG9-1-1 Core Services are not intended to be locally duplicated, but rather utilized as a cross-network resource in support of interoperability and backup capabilities. Additionally, it appears that regional or state level implementation of NG9-1-1 Core Services tend to be more cost effective and provide more opportunities for consistent operations and services to the public as opposed to localized implementations. As the intent of NG9-1-1 implementation is to ultimately interconnect regional, state, and national networks, it is recommended that 9-1-1 Authorities explore regional or state level NG9-1-1 Core Service implementations. Local networks of PSAPs are encouraged to integrate into Regional, State, and National Networks using a transitional plan that best fits their requirements and circumstances. However, it is understood that local regions cannot always readily implement NG9-1-1 functionality due to political, monetary, or operational limitations. The Task Force supports region-specific transitional schedules, which may differ from one another because of the limitations mentioned above. 9-1-1 Authorities at all levels are encouraged to coordinate their planning.
- The TFOPA recommends 9-1-1 Authorities explore the use of a shared infrastructure model and embrace strategies to collaborate and share resources when transitioning to NG9-1-1 as a way to meet their responsibility for providing an optimally effective and efficient emergency communications system for their citizens and emergency responders. Having an advocate in favor of the resource sharing is critical when considering sharing 9-1-1 operational procedures and resources. Understanding stakeholder, agency and individual perspectives will be critical to the success of the program.
- There is a need for detailed, consistently measured, specific and well-documented standardized data to support decisions related to how shared governance agreements will be developed and executed. Additional research by the TFOPA is needed to define common elements of PSAP cost, and potential cost savings. Once cost is defined and current sources of funding are identified and understood, it is important to establish the terms of cost sharing that collaborating jurisdictions will utilize.

ARCHITECTUAL/TECHNICAL

- PSAP managers and other 9-1-1 Authority leaders should start to familiarize themselves, if they haven't already, with the technologies and components that make up modern communications and data processing systems. While management personnel do not need to become technical experts, they should begin to investigate and have a basic working knowledge of technical concepts such as Internet Protocol-based networking, client/server computing, server virtualization, and cloud computing. PSAP architecture optimization will build upon the use of several of these enterprise technologies that are utilized within modern computing and communications systems including those employed in Public Safety. Managers will need to have at least a basic understanding of these technology concepts to meaningfully participate in the NG9-1-1 conversation with vendors, regulators and certain technology-savvy sectors of the general public.
- Jurisdictions/9-1-1 Authorities should analyze and consider the following factors as they evaluate the optimization models included in this report for suitability for their own unique environment. Note that this is not an exhaustive list of optimization factors but rather a list of those considered most imperative for use as model evaluation criteria by individual jurisdictions:
    - Financial
    - Interoperability
    - Survivability/Reliability (Operational)
    - Elasticity/ Scalability
    - Security
    - Operational Staffing
    - Service Operations Effectiveness
- The PSAP Managers/9-1-1 Authority leaders must keep in mind that the advantages associated with infrastructure sharing only apply to those infrastructure services and functions that are actually shared. While this report covers the potential deployment models available to PSAP and 9-1-1 Authority management, some of the models definitely involve resource and functional systems sharing across PSAPs and /or jurisdictions and their advantages (and challenges) are clearly delineated. These management teams should undertake clear, purposeful, and painstaking analyses of their individual circumstances with all of the identified advantages and challenges of each deployment model clearly in mind, so that decisions on chosen deployment models are made deliberately with full knowledge. Likewise, the continued reliance on legacy architecture should also be a deliberate choice rather than the result of "institutional inertia."
- Those responsible for NG9-1-1 systems deployment should be looking for ways to drive network interconnection across their jurisdiction and, where possible and necessary, with other jurisdictions. The use of "walled garden" environments may have been a chosen and acceptable architecture in the past, as there were limited use cases for interconnectivity among disparate networks, but today, connectivity between networks is now more the norm than the exception. The end-state of a fully NG9-1-1 environment is a network of network. Optimization results from scale.

Optimal configurations will result from ESInets and NG9-1-1 Core services that are designed and deployed to serve populations that maximize the utilization of the networks and shared NG9-1-1 infrastructure and meet the needs of the served Public Safety Authorities.

- The TFOPA recommends that the ESInet, the NG9-1-1 Core Services functions, and controlling databases be monitored 24x7x365 by a NOC with visibility across the network. (Note that monitoring above the physical network layer may not be part of current NOC responsibilities.) All elements should be alarmed and current network and system diagrams should be available to assess any loss of connectivity or functional performance. This should include a Simple Network Management Protocol (SNMP) system to monitor the devices in the system. Priority should be established for network alarms with service impacts taking top priority. Potential service disruptions such as the loss of redundancy should also be prioritized.
- The ESInet should be secured using state of the art security technology (outlined in standards and best practice documents) that includes appliances and security practices designed to secure, monitor, detect intrusions, authenticate users, mitigate events and recover. Border Control Functions (BCF) functions, including Sessions Border Controllers (SBCs) and Firewalls as discussed in "NENA 75-001 Security for Next-Generation 9-1-1 Standard (NG-SEC)" should be employed to secure ESInet from security threats. Security requirements and practices are more thoroughly addressed within the TFOPA WG-1 report focused on Security.

STANDARDS / BEST PRACTICES

- The integration and transition of end user applications into the NG9-1-1 System Infrastructure should be developed. End user applications will be used as 9-1-1 call origination sources and may include unique interface and security aspects. An industry group is recommended to study the implications of end user application access to NG9-1-1.
- Collaboration and consensus-based forums should be used to develop and finalize voluntary best practices for providing public safety grade NG9-1-1 services. These include examining overall monitoring, reliability, notifications, and accountability in NG9-1-1 environments, which should be accomplished in an appropriate and timely manner.
    - The focus of this collaborative effort should be to develop and implement processes in the evolving NG9-1-1 environment to (1) *Identify* risks that could result in disruptions to 9-1-1 service; (2) *Protect* against such risks; (3) *Detect* future 9-1-1 outages; (4) *Respond* to such outages with remedial actions, including notification to affected 9-1-1 Authorities, and (5) *Recover* from such outages on a timely basis in cooperation with any affected subcontractors.[92] These five elements, although taken from National Institute of Standards and Technology NIST documents, have always been fundamentally applicable to overall 9-1-1 service management.
    - Recognizing that the implementation of best practices may obviate the need for additional rules beyond those adopted in the FCC's 9-1-1 Reliability Order, a

[92] http://www.nist.gov/cyberframework/index.cfm, last accessed December 2, 2015

consensus based process should recommend any changes believed to be necessary to reflect the emerging NG9-1-1 ecosystem. These recommendations should be consistent with the overarching goals of encouraging innovation and investment in NG9-1-1 and avoiding duplicative regulatory requirements.

- Best practices should also be developed for contract provisions between state and local public safety agencies and their 9-1-1 service providers to facilitate NOC functionality and other enhanced services that would promote reliability.
- As with all best practices, the collaborative work of this consensus body should also be flexible to account for differences in the financial and personnel resources available to individual PSAPs, state and local governments, and 9-1-1 Service Providers, as well as differences in the legal and governance environments in which 9-1-1 services are provided.
- Efforts should be made to accelerate the continued development and implementation of NG9-1-1 standards and systems, while assuring reliability.

EDUCATION / TRAINING

- The implementation of NG9-1-1 technology will require significant training, re-training and recurring supplemental training and education through the transition into the end state of the technology implementation. This training will not be limited to PSAP and 9-1-1 Authority operations personnel, but should also include personnel from those public safety agencies that receive services from the PSAP.
- Comprehensive outreach and education for both 9-1-1 stakeholders and the public is critical to the effectiveness and overall acceptance of all aspects of NG9-1-1. PSAPs, the public safety community, and their governmental entities must fully communicate the challenges, the needs and requirements of the envisioned transition including the identification of adequate capital and sustainment funding of the transitional and end state NG9-1-1 technology implementation.
- PSAPs, the public safety community, services and equipment providers, policymakers, and the public need to know more about and remain informed of the impending transition to NG9-1-1 technologies and how it is impacting public safety communications and the provision of services by PSAPs. Comprehensive outreach and education for both 9-1-1 stakeholders and the public is critical to the effectiveness and overall acceptance of all aspects of NG9-1-1. PSAPs, the public safety community, and their governmental entities must fully communicate the challenges, the needs and requirements of the envisioned transition including the identification of adequate capital and sustainment funding of the transitional and end state NG9-1-1 technology implementation. As early adopters across the nation implement their NG9-1-1 networks and advanced capabilities, ample lessons learned and successful achievements abound and can be used to further design and implement programs, practices, and methods to successfully and effectively deploy NG9-1-1.

7.3 Optimal Approach to Next-Generation 9-1-1 Resource Allocation for PSAPs

Without question, 9-1-1 systems provide a crucial benefit to all of society, yet the governance and funding of the 9-1-1 system pose a challenge. Unfortunately, current methods of recovering the costs of 9-1-1 systems across multiple jurisdictions are a complex hodgepodge of approaches. Existing fee collection mechanisms are arguably outmoded. Many contend they must be updated to be more equitable, consistent, and sustainable. The Task Force shares the view of many in the public safety community that *any* technology or services capable of accessing the 9-1-1 system should contribute its fair share to operate the legacy 9-1-1 systems and also to assist in the build-out of NG9-1-1 networks. With that in mind, TFOPA offers the following conclusions and recommendations to help address NG9-1-1 resource allocation for PSAPs and supporting 9-1-1 Authorities:

- As a matter of public policy, 9-1-1 funding must be predictable, stable, and dedicated only for that purpose. A 9-1-1 user based fee shall be assessed monthly in a competitively neutral manner on all technologies utilized to place a 9-1-1 emergency request for assistance to a public safety answering point through an emergency communications network. Such fee can include a traditional fee on an access line or communications device in a subscription, an amount in a pre-paid wireless plan, or going forward, could be assessed on user broadband connection to an internet access network provider.
- Based on a review of previous studies on funding 9-1-1, it appears that a cohesive, strong statewide 9-1-1 planning and coordinating mechanism is necessary in all states to facilitate the timely and efficient deployment of NG9-1-1 networks.
- The quality and accuracy of 9-1-1 data at all levels of government can be improved. Better and complete data on all aspects of 9-1-1 funding will facilitate federal and state efforts to set appropriate and sustainable levels of funding for this critical public service.
- The concept of "cooperative federalism" must be the foundation governing the transition of existing 9-1-1 networks to NG9-1-1. Statutory authority over 9-1-1 exists at both the state and regional levels and in certain regulatory environments the FCC maintains jurisdiction. 9-1-1 calls, which necessarily almost always begin and terminate within a State/jurisdiction are *by definition* clearly both intrastate and subject to State oversight.
- The NG9-1-1 systems require that shared services networked across multiple PSAPs meet a series of well-defined conventional criteria. However, such criteria should be established by a state or regional governing body and include decision analysis, cost effectiveness, budgetary constraints and priorities, accountability, and a well-defined governance structure, subject to external audits and contractual obligations.
- The consolidation of PSAPs does not necessarily translate into increased efficiencies or cost savings. With that in mind, this report focuses more on which funding mechanisms offer the best approach going forward in light of the policy principles mentioned earlier.
- Changes to the current 9-1-1 funding model should be considered that would include 9-1-1 fees on end user broadband services including the examination of a "network

connection" fee that would be assessed on all facilities-based service providers enabling access and communicating with public safety.

- Addressing prepaid wireless plans is a crucial part of assuring sustainable and technologically/competitively neutral 9-1-1 funding. The TFOPA encourages states that have yet to address this issue to resolve this "funding gap" as quickly as possible through state legislation. As more data on actual collections is developed by state entities, and compared to forecasted collection for this class of customers, this issue will need more scrutiny. The TFOPA recommends that the FCC should refer a more detailed examination of this issue to the joint advisory committee recommended below.
- Studies of 9-1-1 fees and NG9-1-1 deployment should be developed with a strong emphasis towards implementation and execution. In particular, a much more integrated, intensive approach toward outreach and education must be developed for the 9-1-1 community.
- A Local State Government Advisory Committee should be convened to focus on NG9-1-1 issues. The goals of such a committee would include the development of messaging points and information for local, state and federal entities to understand NG9-1-1, funding and policy recommendations and more.

Appendix 1 – PSAP Cybersecurity Use Cases[93]

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 Central Processing Unit (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.

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

[93] 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.

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 cybersecurity infrastructure, this particular scenario could have severe and potentially deadly impacts over an indefinite period of time. With proper planning, capabilities and, most importantly, a well-trained and knowledgeable staff, the impacts can be lessened.

Based on current configurations in the majority of 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 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 date 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 PBXs

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 PBXs 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 PBXs.

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.)
- PSAP#1 staff, PSAP#2 staff, PSAP#3 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 Multimedia Messaging Service (MMS) messaging to the PSAP.

1. PSAP#1 receives a spoofed MMS text message from the orchestrator via the OSP and TCC
2. PSAP#1 staff view the video file unknowingly executing the malicious code. PSAP#1 due to weak cybersecurity measures has now been compromised.
3. PSAP#1 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. PSAP#2 systems begin to have failures and problems with call handling functions.
6. PSAP#3's cybersecurity monitoring and security measures detect the malicious codes attempt at access alerting PSAP#3 staff.
7. PSAP#3 staff investigates the alarms, identify the potential threat, and then enact appropriate plans which include disabling of connectivity to PSAP#1 and eventually PSAP#2.
8. PSAP#3 staff notifies PSAP#1 and #2 of the activity they have identified.
9. PSAP#1 and #2 begin their own actions towards mitigation.
10. Eventually once all systems have been cleaned and tested connectivity to the ESInet 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 cybersecurity measures in place at the originating site and the interconnected sites. Callhandling 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 demilitarized zones (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 cybersecurity 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 cybersecurity planning and additional security measures as indicated in this document which are deemed to fit your cybersecurity model.

Use Case #4: SWATTING Attack.

Prelude

With the transition to NG9-1-1, it may also be possible to directly provide false location information along with the call, as described in [RFC7378]. In addition, cyber-attacks have occurred 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
- First 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. First Responders travel to false location or locations leaving depleted resources available to respond to where the orchestrator's criminal action is taking place.
6. First Responders arrival on scene creates possible chaos or undue attention to the un-expecting individuals at the false locations. This potential chaos or undue attention could create its own set of new calls to PSAPs.
7. First 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:

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. Sub-networks that are physically or logically separated from internal networks, 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).

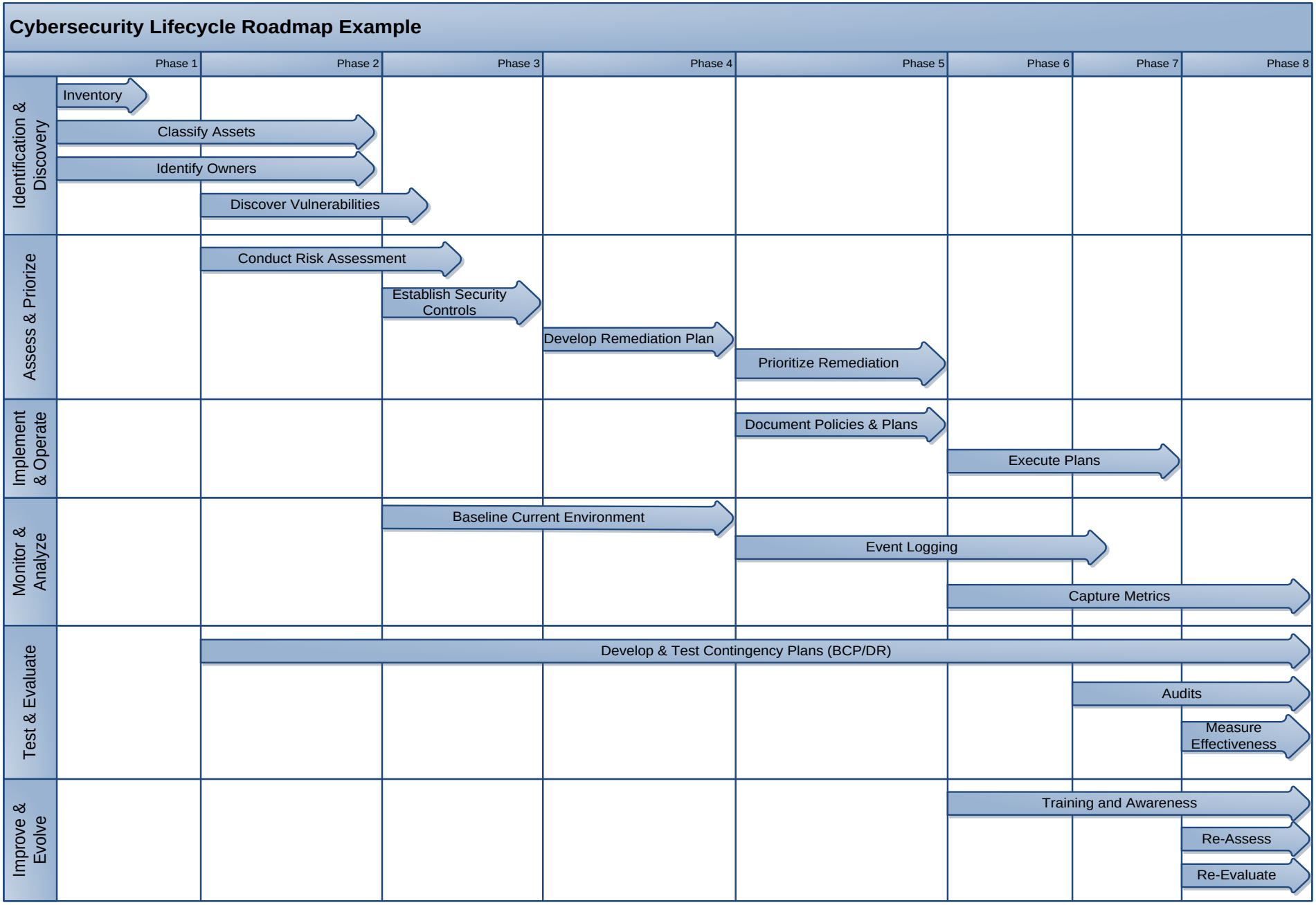
Phase 4 – Organizations should now have completed their initial risk assessment and identified a set of security controls intended to address vulnerabilities and identified risks. This allows the organization to develop a formal and documented remediation plan (2.c) while they continue to baseline their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


Cybersecurity Lifecycle Roadmap Example
Phase 1
Phase 2
Phase 3
Phase 4
Phase 5
Phase 6
Phase 7
Phase 8
Identification & Discovery
Inventory
Classify Assets
Identify Owners
Discover Vulnerabilities
Assess & Priorize
Conduct Risk Assessment
Establish Security Controls
Develop Remediation Plan
Prioritize Remediation
Implement & Operate
Document Policies & Plans
Execute Plans
Monitor & Analyze
Baseline Current Environment
Event Logging
Capture Metrics
Test & Evaluate
Develop & Test Contingency Plans (BCP/DR)
Audits
Measure Effectiveness
Improve & Evolve
Training and Awareness
Re-Assess
Re-Evaluate

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") 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: • 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> • 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> • 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.

	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.
Segmentation	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.
	All wireless networks and infrastructure should be isolated from protected internal networks as if they are an external and untrusted network environment.
	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.
	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.

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); and • Source and destination network address (e.g. - IP address).

	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.

	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.
Development & Change	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.)
	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.)
	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.
	Development processes should ensure that: • 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%200_20111202_0.pdf

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

Appendix 4 – Definitions (Section 5)

9-1-1 Authority: A State, County, Regional or other governmental entity responsible for 9-1-1 service operations. For example, this could be a county/parish or city government, a special 9-1-1 or Emergency Communications District, a Council of Governments or other similar body. Note that various types of responsibilities may apply, such as funding, planning, management, and/or operations of certain service components.

9-1-1 General Roles and Responsibilities: While there are many variations on roles between 9-1-1 Authorities at local, regional, and state levels (including some areas where none of the three formally exist), when viewed at a national level, there is a gradual trend toward the roles and relationships depicted in Figure 1-3 as NG9-1-1 work proceeds. The 9-1-1 Authority term is somewhat generic, as the name of organizations that fill that role vary greatly, such as 9-1-1 Administrator, Emergency telephone Service Board (ETSB), etc. In many cases, the regional or state 9-1-1 Authority does not have direct governance over the local 9-1-1 Authorities. As this report discusses, referencing the roles instead of just the `things' is one way to more clearly state relationships in the 9-1-1 environment.

9-1-1 System Service Provider: the operational and management entity that provides and runs the central 9-1-1 core services components.

Client-Server: Modern data processing and communication systems utilize this model in which client software deployed at the user end point (in the public safety context, usually at a PSAP Telecommunicator position) works in conjunction with server software deployed in an on-premise data equipment room or a shared infrastructure data center. The server-side implementation of client-server deployment is typically called a software service.

Cloud Virtualization: Technology taken to a larger scale where virtual machines / containers can be created for software services in an on-demand fashion within a private government intranet "cloud" or an internet-accessible public "cloud" of computing hardware and storage; cloud technology improves infrastructure usage efficiency and service reliability, provides elasticity to offered load to support peak demands.

Container technologies: An approach to virtualization in which the virtualization layer runs as an application within the operating system (OS).

Data Center Options: Options for the data center infrastructure for PSAPs including the facilities equipment.

- **Government owned and managed** - the data center is owned and managed by the PSAPs or PSAP government.
- **Vendor owned and managed** - the data center is owned and managed by a vendor.

DDOS: Distributed Denial of Service, an attack using mass amounts of access attempts in an effort to slow or bring a system down.

Financial Acquisition Options: Options for the purchase of customer premise equipment.

- **Non-Recurring Cost (NRC)** - charges or fees which only occurred one time. Also referred to as Capital Expenditure (CAPEX).

- **Recurring Cost (RC)** - a regularly occurring cost or estimated cost. Also referred to as Operating Expense (OPEX).

Interlocal: As in Interlocal Agreement, meaning an agreement among local governmental entities for mutual aid and support for emergency operations.

Implementation: Options for the implementation and distribution of customer premise equipment.

- **Geo-diversity** - short for geographic diversity and means physical separation between the primary and backup customer premise equipment. When a system is said to be geo-diverse, operations can continue after a total loss of the primary CPE as the backup is offsite and able to perform all the functions the primary performed.
- **Virtualization** - use of a virtual machine/server/or network vs. a physical machine/server/network router through the use of software emulation or configuration. Multiple virtual machines/servers can be run on a single physical machine/server, allowing a PSAP to use a single machine/server provide several functions. Multiple networks can be configured and administered on a single network router.

Infrastructure as a Service (IaaS): A form of cloud computing that uses virtualized computing resources over the Internet or a private network.

Internet Protocol (IP): Internet Protocol-based networking is foundational to NG9-1-1 and the ESInet WAN and PSAP LAN. The multimedia capability, interoperability, scalability and robustness of the technology that underlies the Internet are leveraged in NG9-1-1 by the use of IP-based networks and communications systems.

IPSR: IP-based Selective Router, typically a softswitch and programming to replace the traditional telephone switch based E9-1-1 Selective Router. The IPSR and an IP network between it and PSAPs allows for reduced costs compared to the traditional switch and analog or digital trunking.

LoST: IETF term meaning Location to Service translation, used in NG9-1-1 in the form of the ECRF, which identifies from the presented caller location which PSAP is normally to receive the call.

NGCS: NG9-1-1 Core Services, the functional components of the central NG9-1-1 process between the OSE and PSAP environments

- **Border Control Function (BCF)**: Provides a secure entry into the ESInet for emergency calls presented to the network. The BCF incorporates firewall, admission control, and may include anchoring of session and media as well as other security mechanisms to prevent deliberate or malicious attacks on PSAPs or other entities connected to the ESInet.
- **Location Validation Function (LVF):** Ensures that a civic address can be used to properly route a 9-1-1 call to the correct PSAP. A functional element in an NGCS that is a LoST protocol server where civic location information is validated against

the authoritative GIS database information. A civic address is considered valid if it can be located within the database uniquely, is suitable to provide an accurate route for an emergency call and adequate and specific enough to direct responders to the right location.

- **Policy Routing Function (PRF)**: That functional component of an Emergency Services Routing Proxy that determines the next hop in the SIP signaling path using the policy of the nominal next element determined by querying the ECRF with the location of the caller. A database function that analyzes and applies ESInet or PSAP state elements to route calls, based on policy information associated with the next-hop.
- **Network Options:** Options for the deployment of the customer premise equipment network (within the PSAP, excludes the ESInet).
- **Government owned and managed** - the network and network equipment is owned and managed by PSAP resources (ex. PSAP IT staff).
- **Vendor owned and managed** - the network and network equipment is owned and managed by a vendor.

PSAP: Public Safety Answering Point (PSAP), may be called a 9-1-1 Center. Where 9-1-1 requests are answered, evaluated, and processed to determine whether dispatch of field responders is needed, and in what form.

Session Initiation Protocol: Is a communications **protocol** for signaling and controlling multimedia communication sessions. The most common applications of **SIP** are in Internet telephony for voice and video calls, as well as instant messaging, over Internet Protocol (IP) networks.

System Maintenance: Options for handling system support such as installation, configuration, monitoring, upgrading, and troubleshooting of customer premise equipment.

- **Government operated and managed** - Customer premise equipment is maintained and managed by PSAP resources.
- **Vendor operated and managed** - Customer premise equipment is maintained and managed by vendor resources.

Server Virtualization Software technologies: Including virtual machine and emerging container technologies that allow multiple applications to share a common server hardware and storage platform.

Software as a Service (SaaS): Software licensing and delivery model in which software is licensed on a subscription bases and is centrally hosted. Sometimes referred to as "on-demand software".

OSE: Originating Service Environment, a term coined to represent various forms of call, message, and data originating entities facing the calling customer, such as OSPs, Access providers, PBX provider/operators, and Smartphone application originators

XDoS: XML denial-of-service attack (XDoS attack) is a content-borne denial-of-service attack

whose purpose is to shut down a web service or system running that service. A common XDoS attack occurs when an XML message is sent with a multitude of digital signatures that uses up computer time to try to validate.

Appendix 5 – Acronyms (Section 5)

Acronym	Acronym Term
1G	First Generation (1G)
ACD	Automatic Call Distribution
ADA	Americans with Disabilities Act
ALI	Automatic Location Identification
ANI	Automatic Number Identification
BCF	Border Control Functions (BCF)
CAD	Computer Aided Dispatch
CAMA	Centralized Automatic Message Accounting
CIDB	Customer Information Data Bases
CPE	Customer Premise Equipment
CPE	Call Processing Equipment
CSRIC	Communications Security, Reliability and Interoperability Council's
DBMS	Database Management System
DNS	Domain Name Service (DNS)
DNS	Directory Name Service
ECRF	Emergency Call Routing Function
EMD	Emergency Medical Dispatch
EMS	Emergency Medical Services
ESInet	Emergency Services IP transport network
ESN	Emergency Services Numbers
ESRP	Emergency Services Routing Proxy
FACA	Federal Advisory Committee Act
FCC	Federal Communications Commission
FE	Functional Elements
GAATN	Greater Austin Area Telecommunications Network (GAATN)
GIS	Geographic Information System
HVAC	Heating, Ventilating, and Air Conditioning
IaaS	Infrastructure as a Service
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
IPSR	IP Selective Router
IRR	Instant Recall Recorder
LAN	Local Area Network
LATA	Local access and transport area
LEC	local exchange carrier
LIS	Location Information Servers
LMR	Land Mobile Radio
LNG	Legacy Network Gateway
LoST Protocol	Location-to-Service Translation Protocol
LPG	Legacy PSAP Gateway
LSRG	Legacy Selective Router Gateway

LTE	Long Term Evolution
LVF	Location Validation Function
MIS	Management Information System
MOUs	Memorandum of Understanding
MPC	Mobile Positioning Center
MSAG	Master Street Address Guide
NCMEC	National Center for Missing and Exploited Children
NEMSIS	National Emergency Medical Services Information System
NENA	National Emergency Numbering Association
NG9-1-1	Next Generation 9-1-1
NGCS	Next Generation Core Services
NIST	NIST
NOC	Network Operating Centers
OSE	Originating Service Environments
OSP	Originating Service Providers
P25	Project 25
POS	Point of Sale
PRF	Policy Routing Function
PSAP	Public Safety Answering Points
PSTN	Public Switched Telephone Network
PTSD	Post-Traumatic Stress Disorder
QA	Quality Assurance
QC	Quality Control
QOS	Quality of Service
RFC	Request For Comment
RMS	Records Management System
ROI	Return-on-Investment
SaaS	Software as a Service
SBC	Sessions Border Controllers
SLA	Service Level Agreements
SNMP	Simple Network Management Protocol
SO	Subscriber Service Order
SOP	Standard Operating Procedures
SR	Selective Routing
SR	Selective Router
SRDB	Selective Routing Database
SS7	Signaling System 7
TDM	Time-division multiplexing
TFOPA	Task Force on Optimal PSAP Architecture
TN	Telephone Number
URI	Uniform Resource Identifier
USPS	US Postal Service
VMM	Value Measuring Methodology (VMM)
VoIP	Voice over Internet Protocol
VPC	VoIP Positioning Center
VSPs	VoIP service providers (VSPs)
WAN	Wide Area Network

Appendix 6 – References for Additional Information Figures

Name	**Title**	**Organization**	**Location**	**Email**	**Phone**
Bill Buchholtz	Executive Director	Bexar Metro 9-1-1 District	San Antonio, Texas	bill@bexarmetro.com	210-408-39-1-1
Kevin Carver	Deputy Director	Licking County Regional Communications Center	Licking County, Ohio	kcarer@lcounty.com	
David Ruton	Technical Coordinator	Licking County Regional Communications Center	Licking County, Ohio	druton@lcount.com	
Frank DelVecchio	Director	Bergen County Public Safety Operations	Bergen County, New Jersey	delvecchio@bcpsoc.com	201-785–8510
Patti West	9-1-1 Emergency Communication Manager	Boulder County Regional PSAP	Longmont, CO	patti.west@longmontcolorado.gov	303-651-8550
Gary Johnson		Upper Peninsula 9-1-1 Authority	Marquette County, Michigan	gjohnson@mqtco.gov	906-475-1196
Ms. Thalia Burns	Communications Manager	Honolulu Police Dept.	Honolulu	tburns@honolulu.gov	
		Harris County 9-1-1 District, Texas	Harris County, Texas	Info@9-1-1.org	832-237-99-1-1
Maria Jacques	Program Director	State of Maine 9-1-1 Program	State of Maine	Maria.Jacques@maine.gov	
Chuck Spalding	9-1-1 Director	Palm Beach County, Florida	Palm Beach County, Florida	CSpalding@pbcgov.org	561.712.6339
Mark Tennyson	State 9-1-1 Program Manager	Office of Emergency Management		mark.tennyson@state.or.us	503-378-29-1-1 Ext: 22265

Appendix 7 - Previous Studies and Analyses

1. National Association of 9-1-1 Administrators (NASNA), June 2015, "**Four Potential Sustainable Funding Models for NG 9-1-1.**" Pub. Evelyn Bailey Consulting, LLC (EBC).
2. National 9-1-1 Office (9-1-1.gov), December 2013, **"Blue Ribbon Panel on 9-1-1 Funding, Report to the National 9-1-1 Program"**, Washington D.C., Pub. Department of Transportation.
3. National 9-1-1 Office (9-1-1.gov), March 2013, **"National 9-1-1 Program, Current State of 9-1-1 Funding and Oversight"**, Washington D.C., Pub. Department of Transportation.
4. East Carolina University (ECU), College of Business, 2014, **"Federalism in the Financing of 9-1-1"**, Greenville, North Carolina, Pub. Bureau of Business Research.
5. Public Safety and Homeland Security, Federal Communications Commission, December 31, 2013, **"Sixth Annual Report to Congress on State Collection and Distribution of 9-1-1 and Enhanced 9-1-1 Fees and Charges"**, Washington D.C., Pub. FCC.
6. National Emergency Numbering Association (NENA), March 2010, "**Next Generation 9-1-1 Transition Policy Implementation Handbook**", Washington D.C., Pub. NENA.
7. National Emergency Numbering Association (NENA), March 2007, "**Funding 9-1-1 the Next Generation",** Washington D.C., Pub. NENA.
8. Dr. Walt Magnuessen, 2014, **"The Status of NG9-1-1 Deployment in the United States"**, iCERT Industry Council for Emergency Response Technologies, Pub. Texas A&M University.
9. East Carolina University (ECU), College of Business, Bureau of Business Research, 2013, **"Next Generation 9-1-1: When technology drives public policy"**, Management Information Systems, Volume 4, Raleigh, N.C., Pub. International Journal Business Continuity and Risk Management.
10. North Carolina 9-1-1 Board, January 6, 2010**, "A report on findings and recommendations on 9-1-1 costs and funding models for the North Carolina 9-1-1 system",** Raleigh, N.C., Pub. North Carolina Board.
11. James Holloway and Elaine Seeman, 2012, "**How non-voice access technology is driving the creation of federal and state NG9-1-1 service and IP enabled communications network policies",** Temple Journal of Science, technology, and environmental law, Philadelphia, PA, Pub. Temple University Beasley School of Law.
12. North Carolina 9-1-1 Board, February 2013, **"Biennial Report to the Governor Joint Legislative Commission on governmental operations, revenue laws study committee"**, Raleigh, N.C., Pub. North Carolina Board.
13. National Conference of State Legislatures, 2014 **"Funding and Governance for 9-1-1 for the National Conference of State Legislatures,**" Washington D.C., Pub. NCSL.

14. The Wireless Association (CTIA), 2014, "**Prepaid Point of Sales Status**", Washington D.C., Pub. CTIA.
15. Federal Communications Commission, 2012, **"Report to Congress on State Collection and Distribution of 9-1-1 and Enhanced 9-1-1 Fees and Charges"**, Washington D.C., Pub. FCC.
16. Public Safety and Homeland Security Bureau, Federal Communications Commission, 2011, **"White paper: A Next Generation Cost Study, A Basis for Bringing Nationwide Next Generation 9-1-1 Networks to America's Communications Users and First Responders",** Washington D.C., Pub. FCC.
17. Federal Communications Commission, 2012, **"Report to Congress on State Collection and Distribution of 9-1-1 and Enhanced 9-1-1 Fees and Charges"**, Washington D.C., Pub. FCC.
18. National 9-1-1 Office (9-1-1.gov), March 2013, **"National 9-1-1 Program, Current State of 9-1-1 Funding and Oversight"**, Washington D.C., Pub. Department of Transportation.