NENA Managing & Monitoring NG9-1-1 Information Document

Abstract: This document provides guidance to 9-1-1 Authorities at all levels, and to their vendors, on considerations and best practices for monitoring and managing NG9-1-1 services and infrastructure. The document covers end-state NG9-1-1 deployments and transitional deployments moving toward full NG9-1-1 functionality. This document contains information and advice; it does not contain requirements or specifications. The document is separated into two sections: one for state, province or regional authorities, and one for responding agency authorities like Public Safety Answering Points and Emergency Communication Centers.

NENA Managing & Monitoring NG9-1-1 Information Document

NENA-INF-040.1-2020
DSC Approval: 06/09/2020
PRC Approval: 07/31/2020
NENA Board of Directors Approval: 08/19/2020
Next Scheduled Review Date: 08/19/2025

Prepared by:
National Emergency Number Association (NENA) Agency Systems Committee, Monitoring and Managing NG9-1-1 Working Group

Published by NENA
Printed in USA

1 Executive Overview

This document provides guidance to 9-1-1 Authorities at all levels (including, but not limited to, PSAPs, State, Regional, Tribal, Provincial 9-1-1 Authorities and other entities that provide infrastructure support for 9-1-1 agencies) on considerations and best practices for adoption in managing and monitoring Next Generation 9-1-1 (NG9-1-1). The topics covered are comprehensive and general guidance is given to assist Authorities in planning for NG9-1-1 as the Authority transitions from legacy 9-1-1 to a full implementation of NG9-1-1. Where appropriate, the document refers to other references to provide additional specific detailed information for use by the 9-1-1 Authority. The intent of this document is to also allow Authorities to apply the guidance even if an Authority is only partially implementing portions of NG9-1-1 in a transitional process on its way to full NG9-1-1 (See Section 2.6.11).

This document provides guidance in categories such that some sections of the document apply to a 9-1-1 Authority at any level (e.g., Security Monitoring and Management). Other sections of the document are specifically relevant only to 9-1-1 Authorities at the State, Province or Regional Level (Section 2.6). There are specific portions of the document (Section 2.7) that contain additional guidance that is most relevant to 9-1-1 Authorities at the PSAP level.

Table of Contents

NENA
INFORMATION DOCUMENT
NOTICE

This Information Document (INF) is published by the National Emergency Number Association (NENA) as an information source for 9-1-1 System Service Providers, network interface vendors, system vendors, telecommunication service providers, and 9-1-1 Authorities. It is not intended to provide complete design or operation specifications or parameters or to assure the quality of performance for systems that process such equipment or services.

NENA reserves the right to revise this Information Document for any reason including, but not limited to:

- Conformity with criteria or standards promulgated by various agencies;
- Utilization of advances in the state of the technical arts; and
- Reflecting changes in the design of equipment, network interfaces, or services described herein.

This document is an information source for the voluntary use of communication centers. It is not intended to be a complete operational directive.

It is possible that certain advances in technology or changes in governmental regulations will precede these revisions. All NENA documents are subject to change as technology or other influencing factors change. Therefore, this NENA document should not be the only source of information used. NENA recommends that readers contact their 9-1-1 System Service Provider (9-1-1 SSP) representative to ensure compatibility with the 9-1-1 network, and their legal counsel to ensure compliance with current regulations.

Patents may cover the specifications, techniques, or network interface/system characteristics disclosed herein. No license expressed or implied is hereby granted. This document shall not be construed as a suggestion to any manufacturer to modify or change any of its products, nor does this document represent any commitment by NENA or any affiliate thereof to purchase any product whether or not it provides the described characteristics.

By using this document, the user agrees that NENA will have no liability for any consequential, incidental, special, or punitive damages arising from use of the document.

NENA's Committees have developed this document. Recommendations for change to this document may be submitted to:

National Emergency Number Association
1700 Diagonal Rd, Suite 500
Alexandria, VA 22314
202.466.4911 or commleadership@nena.org

NENA: The 9-1-1 Association improves 9-1-1 through research, standards development, training, education, outreach, and advocacy. Our vision is a public made safer and more secure through universally available state-of-the-art 9-1-1 systems and better-trained 9-1-1 professionals. Learn more at nena.org.

Intellectual Property Rights (IPR) Policy

NOTE – The user's attention is called to the possibility that compliance with this document may require use of an invention covered by patent rights. By publication of this document, NENA takes no position with respect to the validity of any such claim(s) or of any patent rights in connection therewith. If a patent holder has filed a statement of willingness to grant a license under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license, then details may be obtained from NENA by contacting the Committee Resource Manager identified on NENA's website at https://www.nena.org/ipr.

Consistent with the NENA IPR Policy, available at www.nena.org/ipr, NENA invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement any standards referenced by this document or to implement or follow any recommend best practices, procedures or architectures contained herein.

Please address the information to:
National Emergency Number Association
1700 Diagonal Rd, Suite 500
Alexandria, VA 22314
202.466.4911
or commleadership@nena.org

Reason for Issue/Reissue

NENA reserves the right to modify this document. Upon revision, the reason(s) will be provided in the table below.

Document Number	Approval Date	Reason For Issue/Reissue
NENA-INF-040.1-2020	08/19/2020	Initial Document

2 Best Practices Common to 9-1-1 Authorities at all Levels

This document uses the word "call" to refer to a session established by signaling with two-way real-time media and involves a human making a request for help. We sometimes use "voice call," "video call" or "text call" when specific media is of primary importance. A call can also be initiated by an automaton in order to provide one-way communication of emergency data (e.g., a chemical sensor alerting a PSAP). See "NENA i3 Standard for Next Generation 9-1-1", NENA-STA-010 [2] , for information on non-human initiated calls.

Common terminology for the 9-1-1 industry, as adopted by NENA, is found in the NENA Master Glossary of 9-1-1 Terminology [1] .

2.1 Alert Conditions

Alert Conditions defined in this section are intended to apply to systems operated by all 9-1-1 Authorities. Alerts may take multiple forms (audible, visual, logging, etc.) and should be capable of being directed to 9-1-1 Authority defined destinations (PSAPs, Other Responder Systems, Network Operating Centers (NOC), etc.). These alerts are typically both audible and visible to appropriate responsible personnel while working at their normal work positions. The audio portion of an alert might be switched to a silent mode so that operations are not disrupted, but the visual indication should remain visible as long as the alert (e.g., trouble condition) exists. Outgoing alerts from the agency to the public or other external entities should also be monitored for false alerts.

Alerts should be categorized into a minimum of three Condition States:

- Critical Alert Conditions - Require immediate notifications and immediate response as necessary. A Critical Alert Condition is when a system function, workflow interruption or process problem results in the inability to deliver or handle 9-1-1 calls. Other Critical Alert Conditions include the inability to utilize administrative capabilities to properly manage NG9-1-1 operations including incident handling.
- Major Alert Conditions - Require immediate notifications but may not necessitate immediate response per local policy (e.g., less than 24-hour response). A Major Alert Condition is when a system malfunction, workflow interruption or process problem results in NG9-1-1 call handling being affected to a degree that call answer and/or call handling times exceed normal thresholds set by local policy. A Major Alert Condition can also impact the normal utilization of administrative capabilities (e.g., GIS data uploads or spatial data management change processes are rendered inoperable). Other examples of Major Alert Conditions include voice quality issues, mapping delivery failures, when one part of a redundant system fails, or one PSAP is unable to process and dispatch calls but another PSAP is able to handle the call. Certain quality issues could escalate to a Critical Alert Condition depending on severity.

- Minor Alert Conditions – Require less urgent notifications (e.g., required response by next business day). Minor Alert conditions are all alerts not categorized as Critical or Major. Examples include loss of redundancy for elements that do not threaten continued operations, additional failures that are not service affecting such as a fan in a server, loss of one power supply when dual power supplies are available, or a single disk drive failure in a Redundant Array of Independent Disks (RAID) environment.

Response times, escalation times, and levels of support for each category of Alert Condition should be negotiated in Service Level Agreements (SLAs) between stakeholders (including contractors) based on local requirements, local resources available, and the nature of the Alert Condition. Reporting of issues that do not affect service, such as degradation in redundancy, should be spelled out in an SLA between service providers and the 9-1-1 Authority.

2.2 Network Management Monitoring

All administrators of NG9-1-1 networks and/or vendors who manage NG9-1-1 networks and 9-1-1 Authorities who manage those vendors should familiarize themselves with the Network Management and Monitoring section of the NENA-INF-016, Emergency Services IP Network Design (ESIND) [3] .

The Network Management and Monitoring section of ESIND deals with activities like the use of Quality of Service (QoS) monitoring, Simple Network Management Protocol (SNMP), network performance monitoring, and important aspects of SLAs with network service vendors.

Different entities or authorities could be monitoring different facets of the network components, servers, and applications. In some cases, one entity might monitor all aspects of the infrastructure and overall system. In other cases, separate entities might monitor individual aspects. The 9-1-1 Authority should consider the management structure when negotiating SLAs so that the 9-1-1 Authority receives the necessary reporting information to interact with and manage the network service provider or NG9-1-1 system.

It is critical to have accurate documentation of the network infrastructure to communicate properly and provide effective network management as described in the Network Management and Monitoring section of the ESIND document.

2.2.1 Quality of Service (QoS)

QoS is the measurement of the overall performance of a transport system like an IP network. QoS measurements are extremely important in streaming media applications like voice or video. For example, the administrators may want to be notified when network bandwidth utilization reaches two-thirds of its capacity. NENA-STA-010 [2] specifies the use

of DiffServ to mark traffic in Next Generation Core Services (NGCS) ESInets with different priorities to achieve a certain level of QoS. The different priority levels are called Differentiated Services Code Points (DSCP). Switch and Router statistics for different Code Points should be monitored (e.g., percentages of packets with a given DSCP, overall, and in the worst minute/second) to determine when additional capacity may need to be added. Similar monitoring of usage patterns for different classes of network traffic should be implemented on other networks that are not required to use DiffServ, and that instead use 802.1p and 802.1q for traffic type marking.

2.2.2 Simple Network Management Protocol (SNMP)

SNMP is a mechanism for monitoring network devices, servers, and applications. The SNMP management system may be connected to the device it is monitoring to request device status and to change device parameters. The SNMP management system typically has robust threshold management capabilities. The SNMP management system operator should share information with interested parties (PSAPs, etc.). NENA-STA-010 [2] requires that SNMPv3 is used because of its superior security features. Devices that do not support SNMPv3 should be replaced by devices that do support SNMPv3 as soon as possible.

Devices and applications that support SNMP can be configured to send SNMP traps (alerts) to places where the device or application is to be monitored. SNMP traps could be sent to multiple destinations. SNMP traps could go to the network vendor's NOC depending on what the 9-1-1 Authority desires, and the 9-1-1 Authority could have their own capability to monitor the SNMP traps. Different management hierarchies may require different reporting patterns. To use the SNMP trap functionality, the network element must provide an SMNP trap and there must be an SNMP management system to receive the SNMP trap.

2.2.3 Network Configuration Protocol (NETCONF)

The Network Configuration Protocol, defined in RFC 6241 [4] , is another network management protocol becoming accepted in the network monitoring industry. NETCONF may be used for the devices that support it.

2.2.4 Internet Control Message Protocol (ICMP)

ICMP pinging is a common mechanism used to determine if another device is reachable. The administrator must ensure that firewalls allow the desired ICMP packets to pass. Devices and systems should be configured to respond to ICMP messages.

2.2.5 Test Call Generator Interface

NENA-STA-010 [2] defines a Test Call Generator interface designed to exercise NGCS and PSAP call processing functions and interfaces. OSPs should be encouraged to send test calls to their PSAPs as a normal routine. See the Test Call Generator interface in Section

2.7.6 for background information on the features and functions anticipated for this interface. Frequent test calls with an adjustable frequency are desired and the Call Handling elements should be configurable to expect regular test calls. When a test call fails, an alert can be sent. Such test calls are not answered by a call taker and would be excluded from call processing metrics for performance management. Note that failure of a test call may be caused by failure of network connectivity or equipment, hardware or software (server issue), or failure of a necessary Element or Service.

2.2.6 In-band versus Out-of-band management.

It is advisable for network management systems to use secure dedicated facilities to access critical network elements for all management functions. For example, access to routers should include facilities that do not use the i3 production network, like using routers' console ports. This allows router reconfiguration and recovery when routers cannot be reached over the production network.

In addition, other stakeholders such as vendors, security monitoring groups, and those doing Management Information Systems (MIS) activities may require secure external communication access to the network devices and applications using facilities such as VPN. These requirements and any expected bandwidth should be considered upfront when planning the network design.

Probes may be utilized to provide remote monitoring and management at various points in the network. These probes may conduct active network testing such as pinging and may also provide facilities for remote access to network devices' console ports.

For troubleshooting purposes, the ability to capture network packets is critical. During the initial network design phase, it is advisable to consider how traffic will be captured on the network. Packet capture devices are available that can be used at key points in the network to facilitate troubleshooting when a problem has been detected.

There may be other monitoring applications and facilities available that are not standardized. Some network devices might have proprietary capabilities for analysis that can be utilized. It is advisable to take advantage of any facilities that are available.

2.3 Continuity of Operations Plan (COOP)

With the implementation of NG9-1-1 by a 9-1-1 Authority, planning for continuity of operations when technology fails should not be overlooked, despite the promise of "five nines" availability [19] . At a minimum, regular exercise of COOP plans is encouraged to keep awareness and skills at a high state of readiness so that use of the COOP is a familiar process and leads to successful results when the COOP is activated. 9-1-1 Authorities at all levels may have specific requirements for COOP plans and exercises. The planning of any NG9-1-1 system should be cognizant of those requirements. The 9-1-1 Authority is

encouraged to also consider guidance provided by APCO and NENA to maintain service capability across several areas. Specific targets that should be considered for preparedness, survivability, and sustainability are found in APCO/NENA ANS 1.102.2-2010, Service Capability Criteria Rating Scale [5] The Federal Emergency Management Authority (FEMA) also provides guidance and templates that may be of assistance and can be found at the FEMA COOP website [6] .

In the process of establishing an NG9-1-1 system, the 9-1-1 Authority should exercise some aspects of the COOP on a more frequent basis (such as monthly or quarterly). Examples of where more frequent exercise of COOP would be appropriate to maintain essential skills and awareness might be:

- Incident Handling Systems – A good best practice is to frequently have operations staff do a simulated incident handling system outage and allow staff to track calls and dispatch incidents in a manual mode (using pen and paper and forms). The 9-1-1 Authority should create standardized forms for documenting 9-1-1 information that is reflective of the information documented during normal operations. These forms can be on paper or stored electronically on a localized computer system. Manual forms or computers used for manual operations should be easily accessible in the event of an outage or emergency to ensure COOP. The COOP should include provisions for handling an outage of Records Management Systems (RMS) capability as well.
- Radio Systems – Another best practice is to periodically simulate impairment of radio operations such as where trunked radio capacity becomes unavailable (e.g., by simulating a failure of radio system function). This allows dispatchers to understand failover capabilities of radio systems and also allows first responders to be ready to operate in a situation where radio communications are impaired.
- Policy Routing Rules – Implementation of Policy Routing Rules in NGCS varies among NG9-1-1 system implementations, however, best practice is to establish a recurring pattern to exercise the Policy Routing Rules. In legacy and transitional environments, a PSAP may have a backup ingress network for receiving calls. In this case, the PSAP should develop a comprehensive plan to switch to the backup network as part of a periodic process for testing the COOP. If the PSAP has established inter-jurisdiction agreements in a Memorandum of Understanding (MOU) for receiving calls from another jurisdiction in times of need, an established plan should be followed and regularly exercised to ensure the COOP will work when invoked.

2.4 Security Monitoring and Management

9-1-1 Authorities should proactively secure physical facilities and devices, applications, and network infrastructure. The security status of these assets should always be actively monitored, and processes and procedures for dealing with different types of threats should be documented in advance so that risks to emergency services can be effectively mitigated.

The Department of Homeland Security (DHS) provides advice about "Continuous Diagnostics and Mitigation" (CDM) [7] in the process of assessing security risk and acting to address it. The CDM process involves four phases:

- determining what is on the network
- determining who is on the network
- determining what is happening on the network
- determining how data is protected

These phases should be continually applied in the ongoing process of continuous improvement of an agency's security posture. The DHS website also contains detailed information on protecting against various classes of threats or risks that was developed for federal agency networks. All or most of this information is equally applicable to networks utilized or operated by 9-1-1 Authorities and should be reviewed by those responsible for network and system security.

Security design should be part of an overall system engineering process rather than being imposed on a finished design. Including security in system design allows security principles to be identified and incorporated into the initial design. Degradation or loss of emergency services at an individual PSAP would obviously have a serious impact. Degradation or loss at a State or Regional level would certainly magnify the impact, and this fact should be considered when designing the monitoring and management components of a service continuity risk mitigation plan. This section will identify specific infrastructure elements that should be monitored. Information and requirements for securing these elements are provided in the following documents:

- NENA 04-503, Technical Information Document Network/System Access Security [8]
- NENA 75-001, Security for Next-Generation 9-1-1 Standard [9]
- NENA-INF-015.1-2016, NENA NG9-1-1 Security Information Document [10]
- NENA 75-502, Next Generation 9-1-1 Security Audit Checklist [11]
- APCO document: An Introduction to Cybersecurity – A Guide for PSAPs [12]

- NIST Special Publication 800-160 Vol. 1, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems [13]
- CJISD-ITS-DOC-08140, Criminal Justice Information Services (CJIS) Security Policy Resource Center [14]
- Department of Homeland Security, Continuous Diagnostics and Mitigation (CDM) [7]

2.4.1 General Security Principles

A Security Operations Center or Network Operations Center often has the responsibility of monitoring and managing the security aspects of large network and application infrastructures. Whether a formal center is employed or not, the monitoring and managing activities are necessary. Note that multiple stakeholders may be responsible for managing different aspects of the overall NG9-1-1 infrastructure. It is up to the 9-1-1 Authority to implement methods for adequately monitoring security, assigning responsibility for different aspects of security matters for the different stakeholders, and for mitigating the impact of breaches of the security protections implemented. For example:

- one entity is responsible for physical security of the facility including key cards, locks;
- another entity is responsible for network infrastructure such as access to routers, switches, etc.; and
- a third entity could be responsible for NG9-1-1 agent password authentication.

The 9-1-1 Authority can assign or negotiate on who will be responsible for the various aspects of security aspects of mitigation.

Security infrastructure should be designed such that there are multiple layers of protection, each with one or more monitoring points, so that attempts to breach the protected infrastructure can be detected and dealt with promptly. This "security in layers" principle should be applied to all areas of the agency's plan, from physical security to Cybersecurity and all areas in between. An active program to ensure the security infrastructure is protected should exist and be tested to ensure compliance. Network managers should strongly consider use of Intrusion Detection and Prevention Systems (IDPS) as part of their layered security infrastructure. Intrusion detection systems are capable of monitoring security events for unusual or suspicious activities.

It is important to remember that it is the ability to provide emergency services that needs protecting. All devices, mechanisms, activities, policies, and procedures that are part of the plan should be geared toward protecting the ability to provide those emergency services. Applying this principle along with the "security in layers" principle will help the agency design a better comprehensive security risk mitigation plan.

The statewide or regional ESInet will be connected to multiple PSAPs and/or other ESInets. Therefore, the authorities of these networks have a common interest in securing their emergency services. The statewide or regional authority should establish an interconnection policy that includes policies and provisions for mutual reporting and monitoring. The statewide or regional authority should also assist PSAPs in defining their own security risk mitigation plan. Periodic security audits are required to ensure risk mitigation plans are appropriate, and the statewide or regional authority should also assist PSAPs where necessary with their own security audit. The output or monitoring devices may be shared with stakeholders per a negotiated agreement.

One element of security infrastructure and monitoring is to consider using security threat information from clearinghouses that exist. Among suggested clearinghouses are the following:

- Multi-State Information Sharing and Analysis MS-ISAC Advisory at https://www.cisecurity.org/ms-isac/
- Threatpost.com at https://www.threatpost.com
- Center for Internet Security at https://www.cisecurity.org

2.4.2 Change Control and Security

Following a well thought out process for planning, executing, and documenting changes to network, applications, services, and other infrastructure resources is key to maintaining a secure emergency services environment, and should therefore be a key element of the managing authority's physical and Cybersecurity strategy. The process steps may vary for infrastructure components of different types, but the basic principles of change control are common to all types.

A documented process should govern critical infrastructure change activities, and also detail exactly how an incorrect change is reported and corrected, who corrects it, and who is responsible for managing aspects of the correction process. A change control process is a required element in securing supporting services and resources. A written method or procedure for making changes to these services and resources should incorporate approval and reporting elements to ensure that risks and disruptions of service are properly mitigated. Prior to changes to any critical resource (e.g., database or configuration store), a backup copy should be created and stored as part of the change control process. Any change control process must require that changes are documented in sufficient detail to provide an audit trail usable for forensics in the event of a problem, or for training purposes. There may be other stakeholders that would benefit from this reporting as well. Reporting on the change control process should be considered in SLAs and other management agreements.

2.4.3 Securing Physical Facilities

For regional and state-wide facilities that support multiple PSAPs, the impact of the loss of service is multiplied. Therefore, these facilities and any redundant facilities would warrant greater physical security measures. Securing physical access to buildings, rooms, and restricted storage areas is critical. Multiple levels of security should be designed into the system, beginning at the outer perimeter of the facility, and continuing at each physical level within the facility. NENA 75-001 [9] provides details on the basic requirements for NG9-1-1 security, and the 9-1-1 Authority should incorporate these requirements into the physical security plan.

Securing facilities with physical locks is not enough. Policies and procedures must be in place to ensure that personnel maintain a secure environment. For example, propping a door open effectively neutralizes the security provided by a lock on the door. Controlling the access of non-employees, such as vendors and maintenance personnel, must also be detailed in policies and procedures that are documented and communicated throughout the agency. Securing facilities that house environmental infrastructure like heating, cooling, and power is equally important, and should be included in the physical security risk mitigation plan. For example, loss of power would cause a complete loss of emergency services.

Devices for monitoring lock status, perimeters, and physical areas (i.e. cameras and motion sensors) should be part of the overall risk mitigation solution. Physical barriers that prevent vehicles from ramming or entering the building should be employed at appropriate points on the premises.

The agency must also allocate appropriate human resources for monitoring and managing physical security. Having great monitoring technology in place does no good without trained personnel that can recognize and initiate response to a security breach. Designers of physical security risk mitigation plans should thoroughly review all referenced documents that deal with physical security issues before attempting to design a plan.

2.4.4 Securing Network Infrastructure and Servers

Network security is a key component of the overall security posture. Network routing and switching devices, the servers that reside in the network, and the data traffic that is passed over the network must all be secured. NENA 75-001 [9] describes how the devices and servers shall be secured. NENA-STA-010 [2] describes how the data traffic shall be secured. The specifications in these two documents should be followed rigorously when designing and implementing an IP network and server infrastructure. Additional "best practice" information is contained in the other security documents listed in the References section of this document.

Any device, software, or mechanism that provides an entry point into the network is at potential risk for exploitation. Therefore, points of access that are unrelated to the emergency services mission, such as an IP connected vending machine, should be eliminated wherever possible. All remaining points of access must be carefully controlled and implemented to provide the required security. Some examples would be modems, dual-homed devices, wireless routers or access points, and wired routers, firewalls and gateways. Modems or secondary interfaces to non-emergency-services networks that provide maintenance access to network devices are often necessary, but they introduce risk, and must therefore be carefully secured. Universal Serial Bus (USB) ports should be secured or disabled unless required for system functionality. Unused ports on switches or routers should be disabled. Port security features on switches or routers should be enabled to ensure that unexpected devices cannot plug into a port and access network features.

When designing a security program, identify access points, classify them as to whether they are essential for providing emergency services, eliminate unnecessary ones where possible, and then secure the rest. Regular security audits based on NENA 75-502 [11] will help to identify potential risks. The results of the audit should be used to drive action and training to ensure that security measures are an ongoing priority and that all personnel are aware of the critical nature of unsecured access points.

Physical security of mobile devices is also very important. A lost or stolen mobile device or laptop in the hands of a knowledgeable attacker could provide an entry point into the agency's infrastructure. Measures to remotely control access to, or to delete content, on lost or stolen devices should be implemented. Removable media should be secured with restricted access. Policies should make it clear that securing facilities, sensitive devices, and media is the responsibility of every employee.

2.4.5 Securing Network Infrastructure Devices

Network devices like switches, routers, firewalls, and other appliances that provide the connective infrastructure for the network fabric require special attention. Because they connect various pieces of the network together, they are of particular interest to attackers. An attacker may seek to use these devices as islands to hop between networks of different classes, and which have different security classifications. NENA 75-001 [9] provides important detail on these vulnerabilities, and on how to mitigate them, in the section titled "Layer 2 Security and Separation" proper authentication and authorization mechanisms must be utilized to control access to these devices. Access to the devices' provisioning interfaces should trigger notification to pre-designated management personnel, when supported by the device, so that an attempted intrusion can be detected. Monitoring network traffic levels and failed access attempts are critical to early detection and mitigation of attacks. A pre-arranged process for managing network devices and appliances, for monitoring them, and for responding to suspected attacks should be part of

the 9-1-1 Authority's Cybersecurity risk mitigation strategy. A network management system should be used by the 9-1-1 Authority and/or its service provider for managing and monitoring network devices and securely controlling access, as specified in SLAs. Any SLAs covering this area should include notification and reporting level provisions as agreed to by the parties. See the references section of this document for a list of other applicable standards or information. An appropriate change control process is critical to securing network infrastructure devices. See the Change Control and Security section of this document (2.4.2) for details.

Implementing "high availability" through geographically diverse redundancy is a key component of securing network infrastructure, and of ensuring resiliency and continuation of services when an attack is detected. High availability requirements and strategies are detailed in the "High Availability by Geographic Redundancy" section of NENA 75-001 [9] .

The "Firewalls/Security Gateways" section of NENA 75-001 [9] defines how to secure the network and application infrastructure. Firewalls control the boundary points of the infrastructure and must be utilized on all possible access points. Any unnecessary access points should be eliminated where possible. Simple ACL (Access Control List) rules do not provide enough protection. Application Layer Firewalls are strongly recommended. See NENA 75-001 [9] for details.

NENA-STA-010 defines the BCF (Border Control Function) which incorporates a Session Border Controller (SBC) that is responsible for securing Session Initiation Protocol (SIP) traffic. The BCF is therefore a key element in the security infrastructure, tasked with detecting, reporting, and dealing with SIP-based attacks on the network. The BCF also incorporates a firewall. BCFs and firewalls should be deployed in a layered fashion to ensure that attacks of different types are detected and defended against.

Wireless devices and access points of all types (including Bluetooth®) present important security issues. By nature, they provide easily accessible points of entry to the network and must be properly secured. NENA 75-001 [9] defines specific requirements for wireless device use in an NG9-1-1 system and should be consulted before implementing or modifying any wireless infrastructure that interfaces with emergency services. Deployment of wireless-based monitoring systems that can detect security threats such as unauthorized access and unauthorized devices and access points is recommended. Wireless network managers should consider the deployment of systems that provide a full-time wireless intrusion prevention system (WIPS), wireless intrusion detection system (WIDS) and wireless network (WLAN) security monitoring system that provides dedicated monitoring of the airspace to enable the security, performance, and compliance of WLANs.

The October 2017 disclosure of the "KRACK" WiFi attack [15] highlights another type of attack vector – vulnerabilities in wireless devices themselves. The KRACK vulnerability (short for "Key Reinstallation Attack") affects all types of wireless devices that use WiFi

Protected Access (WPA or WPA2) for security, virtually every Wi-Fi-enabled router, access point, phone, computer, Internet of Things (IoT) or another device. This attack exploits an inherent vulnerability in these wireless security functions that would allow hackers to decrypt, delay, and/or block data traffic, and to inject malicious data or code into network users' legitimate data traffic. To protect from this type of vulnerability, it is important to obtain official patches or updates from each infrastructure device manufacturer and install them as soon as they become available. Any devices that have known vulnerabilities for which no patch or update will be made available should be replaced. In addition, all agencies should follow a few fundamental guidelines:

- Ensure that all client devices are also updated with the latest version and security patches. Replace devices that have vulnerabilities for which no fix will be made available.
- A regular survey of wireless devices should be conducted, and an accurate record kept of all devices and their known coverage areas. Survey both the 2.4 and 5GHz bands, regardless of network configuration, in order to detect connected devices not already captured. The record should be updated when devices are added and should include software and firmware versions. Configuration data should be backed up at the same time.
- For wireless routers and other stationary devices that offer a signal power/range control feature, a range should be selected that is no greater than that necessary to cover the required wireless coverage area.
- Disable 802.11r ("fast roaming") on all multiple access point networks.
- Disable client and repeater functionality on all access points. Consider replacing any repeaters or "extenders" with wired access points.
- Consider requiring endpoint devices to connect via VPN, even when using internal Wi-Fi networks.

More information on the KRACK vulnerability is available at the DHS CISA website [31] including the Department of Homeland Security blog entry from October 2017 [15] .

2.4.6 Securing Applications

The application layer should be secured as one layer of a layered approach to security. Application administrators should identify security functions that require periodic review, and follow the guidelines related to applications in NENA 75-001 [9] . Based on the information gathered in a thorough review, application security functions should be hardened as necessary. External applications from service providers, including those that send and receive data outside of the regular NG9-1-1 data stream, should be vetted and hardened so that they conform to NG9-1-1 security guidelines. Any application permitted

on, or in some way connected to the ESInet is a potential security risk and should be treated as such. All applications should be kept at the most current version and all required patches installed when made available. Applications should be tested for security vulnerabilities and re-tested when updated. When end-of-life announcements are made for an application, the authority should plan for an orderly retirement. Applications should not be extended in use beyond the end-of-life.

NG9-1-1 applications should adhere to the authentication, authorization, and privacy requirements specified in NENA-STA-010 [2] , in addition to following the guidelines in NENA 75-001, Security for Next-Generation 9-1-1 Standard (NG-SEC) [9] .

Generic applications should be implemented and maintained such that they meet the security requirements for applications in NENA 75-001 [9] . If an application cannot be made conformant, the application administrator should consider ways to fix the vulnerability, consider putting the application in isolation, or removing the application altogether.

Applications developed by the authority's in-house efforts must be tested at regular intervals for common security vulnerabilities. Use of deprecated software functions or failure to enforce strong data typing and error/bounds checking can result in serious vulnerabilities to applications and protected data.

Web application security scanners should be used to test for common vulnerabilities in web applications.

2.4.7 Securing Data Traffic

Securing the data traffic that is passing across the ESInet requires several layers of measures that work together. NENA-STA-010 [2] specifies secure mechanisms for authenticating the identity of entities that request authorization to send data across the ESInet (see the "Identity" section of NENA-STA-010 [2] for details). It is important to deploy these identity and authentication mechanisms exactly as specified because all entities connected to the ESInet must be able to rely on the asserted identity of others.

All traffic on the ESInet must be secured with the mechanisms specified in the "Integrity Protection" and "Privacy" sections of NENA-STA-010 [2] In addition, 9-1-1 Authorities should be prepared to upgrade the required integrity protection and privacy algorithms as noted in the "Algorithm Upgrades" section of NENA-STA-010 [2] . Additional detail on privacy algorithms can be found in the "Encryption and PKI" section of NENA 75-001 [9] . The requirements for encryption key management and use of a Public Key Infrastructure (PKI) in NENA 75-001 [9] must also be followed carefully as part of managing the data privacy functionality.

In addition to securing data traffic at the transport level, NENA-STA-010 [2] specifies using the secure versions of several protocols from the Session Initiation Protocol (SIP) suite, including Secure Real Time Protocol (SRTP), Secure Real Time Control Protocol (SRTCP) and SDP Security Descriptions for Media Streams (SDES). See the "Transport" subsection of the "SIP Call" section in NENA-STA-010 [2] for details.

Exceptions generated because a user, application, or service is attempting to circumvent a required security mechanism should be monitored. Procedures for responding to nefarious attempts should be decided in advance so that risk can be limited as much as possible. To ensure that all legitimate data can be delivered, NENA-STA-010 [2] allows "fall back" to alternate security mechanisms that may be somewhat less stringent. Managing secured data traffic requires monitoring these "fall back" occurrences to ensure that an intruder cannot exploit the fall back capability. This monitoring should be a part of the broader activity of monitoring the networks and applications that support the emergency services mission. Risk mitigation plans should include procedures to be followed in the event the fall back procedures are part of a detected intruder's actions.

Data traffic in a data center that houses NGCS might include traffic that is not directly related to the NGCS, or to providing emergency services, but that is necessary for some other business purpose. This traffic should be isolated if possible, either on a separate network, or on a specially secured subnet of the ESInet. The security on such a subnet must be at least as strong as that of the overall ESInet. "Sandbox" functionality can be used to isolate session data and provide an additional layer of protection and should be considered for use when a user needs to connect to a service that is not part of the NG9-1-1 system, such as web site or web service. A sandbox function isolates data that is stored locally during a web session. When the session ends, the session data is deleted, preventing a subsequent web session from accessing it.

Data traffic must be continuously monitored for patterns that could indicate a Denial of Service (DoS) attack. NENA-STA-010 [2] describes mechanisms to be used by a BCF to provide notification of SIP-based DoS attacks. Non-SIP traffic must also be monitored for potential DoS attacks. DoS attacks often involve sending a very high volume of requests to an IP address or addresses but may involve an attempt to exhaust resources other than available network bandwidth, like application server resources. Detecting such attacks requires monitoring the type of requests being received and notifying the appropriate Administrator(s) of unusual patterns. Security audits and test procedures should include simulating known types of DoS attacks to ensure that risks to service can be properly mitigated. Procedures for responding to a suspected attack must be documented in advance, and personnel must be trained to follow the procedures. See NENA 75-001 [9] for information on mitigating risks associated with DoS attacks. All types of DoS attacks must be planned for, including Distributed Denial of Service (DDoS) attacks, and Telephony

Denial of Service (TDoS) [34] attacks. In transitional states, legacy PSAPs may be the target of TDoS attacks through the NGCS.

The United States Computer Emergency Readiness Team (US-CERT), a department within the Department of Homeland Security (DHS), has been alerted to an increase in distributed denial of service (DDoS) attacks using spoofed recursive DNS requests. These attacks are troublesome because all systems communicating over the internet need to allow DNS traffic. The attacks work in the following manner: a malicious attacker sends several thousand spoofed requests to a DNS server that allows recursion. The DNS server processes these requests as valid and then returns the DNS replies to the spoofed recipient (i.e., the victim). When the number of requests is in the thousands, the attacker could potentially generate a multi-gigabit flood of DNS replies. This is known as an amplifier attack because this method takes advantage of misconfigured DNS servers to reflect the attack onto a target while amplifying the volume of packets.

US-CERT has published a paper that discusses DNS recursion, helps users understand more about potential targets and risks, outlines methods for protecting DNS servers, and provides best practices for configuring DNS servers [16] .

2.4.8 Securing Supporting Services and Resources

Because incorrect changes to services and resources like DNS, DHCP, and IP address provisioning can have very serious consequences, changes to any of these should be closely monitored, and should trigger automatic notification to managers at multiple levels. Access to critical network services and resources should be carefully controlled, and there should be clearly delineated areas of responsibility for who will approve changes, who will execute them, and who gets notified of access to, and changes to these services and resources. An appropriate change control process is critical to securing supporting services and resources. See the Change Control and Security section of this document (2.4.2) for details.

Changes to, and attempts to change, supporting services like DNS, DHCP and IP address configuration (and underlying data) are sometimes logged on the server or device housing the service and may be forwarded to a central monitoring facility. Any such monitoring mechanisms should be leveraged as part of the process of securing these critical services and resources.

2.4.9 Securing Access to Data

The "Authorization and Data Rights Management" section of NENA-STA-010 [2] specifies mechanisms used to secure access to data. Unauthorized attempts to access or modify secured data must be continuously monitored, and the appropriate Administrator(s) must be notified of any unusual patterns in such unauthorized attempts. Such monitoring and notification must include data access authorization failures for users, systems, and service

accounts. Data used for provisioning, like system and software configuration data, should be carefully protected and monitored on an ongoing basis. Personal information about agency personnel can be highly sensitive data and should be secured and monitored through similar mechanisms.

NENA 75-001 [9] specifies separation of production systems and data from non-production systems and data and requires use of a proper change control process when moving non-production systems or data to the production environment. See the "Separation of Production from Non-Production Systems" section in NENA 75-001 [9] for details on these requirements, and on how to treat temporary data that may be utilized during outage or recovery procedures.

2.4.10 Security Management Authority

Data such as usernames, passwords, and certificates, which are involved in authenticating users, systems, and applications must be carefully protected and monitored by trusted personnel. The "User Access Management" section of NENA 75-001 [9] provides minimum guidelines for management and administration of user/entity account information. The PSAP Credentialing Agency (PCA) is the root certificate authority for NG9-1-1 and should be utilized as the base of any certificates issued by, or on behalf of, the agency for authentication purposes. Data used in the authentication process must be secured as described in the "Securing Access to Data" section above, and successful and denied attempts to access the data must be monitored. Policies regarding the treatment of authentication-related data must be clearly documented and communicated to all personnel. See the Security section of NENA-STA-010 [2] for details regarding identity, certificates and the PCA. 9-1-1 Authorities should plan for the personnel time and software required to manage security-related data.

2.5 Physical Facilities and External Services

Monitoring and managing the physical facility that houses the NG9-1-1 infrastructure and services, ESInet, and NGCS is as important as managing the network, hardware, and software infrastructure inside. Major areas that should be monitored include:

- Primary power and battery backup power facilities
- Generator power facilities and fuel
- System and data redundancy status
- Environmental conditions for hardware infrastructure, such as temperature and humidity
- Fire alarm maintenance and testing
- Water detection alarms

- Flood protection infrastructure
- Physical security infrastructure, such as biometric access controls, CCTV surveillance, guards, man traps. See the Securing Physical Facilities section of this document (2.4.3) for details
- Services that support facility staff, like water supply and air conditioning/heating facilities as human requirements will differ from those required for housing hardware
- Alerts and notifications (should be proactively monitored per policy)
- National Weather Service alerts
- Service provider connectivity (phone, WAN, etc.)

See the Securing Network Infrastructure section of this document (2.4.4) for more information.

Sensors with automated notification capabilities should be employed if available and should be supplemented by human monitoring procedures as needed. Emerging technologies like Artificial Intelligence systems that provide monitoring decision assistance and analytics capabilities should be investigated where available. Responsibilities and processes for monitoring, notification, and reporting should be documented in advance. An SLA that specifies detailed requirements, responsibilities, and processes is required for any monitoring and/or management of physical facilities and external services that is performed by any outside entity.

Managing physical facilities requires complete and up to date as-built schematics and proper labeling of cabling and equipment. Regularly scheduled tests of all backup systems and failover mechanisms should be conducted to ensure that fail-safe facilities are functioning properly.

The ANSI/TIA-942 Standard [17] is a quality standard for data centers. A state, regional or provincial data center housing NGCS infrastructure should follow the requirements and guidelines for a data center hosting services for multiple tenants as defined in ANSI/TIA-942 [17] . Technical experts from the 9-1-1 Authority should familiarize themselves with this standard and require vendors operating NGCS data centers to describe in an SLA how they will meet and/or deviate from the specifications therein.

Some recommendations in NENA's PSAP Site Characteristics Information Document, NENA-INF-024 [18] are also applicable for data centers that house NGCS systems and should be reviewed along with IT industry best practices when preparing sites for NGCS deployments.

2.6 State/Province/Regional Agency Responsible for NG9-1-1 Core Services

2.6.1 Introduction

Authorities that operate all or part of NGCS system, or the ESInet on which it resides, are responsible for elements of the delivery of calls and/or data to PSAPs and other NGCS systems. Service status at this level affects not only downstream entities like PSAPs, but also peer entities that operate other NGCS systems. Service status should be shared among responsible designated authorities.

Managing an NGCS system requires a significant amount of system status monitoring at many levels, from the environment and supporting services, to the network equipment and servers, to the application services that comprise the NGCS. Those who are physically managing these systems will likely be responsible for monitoring their stability and for reporting to the designated authority management. The authority management will typically report status to dependent agencies and entities. Entities operating elements of the NGCS may be contracted or outsourced. In the case where a 9-1-1 Authority is physically managing the NGCS system, the monitoring activities are the same but the reporting paths may differ. Regardless of governance model, the things that should be monitored remain the same, as does the need to inform downstream entities of service status and to be informed by upstream entities of the status of their services.

2.6.2 Characteristics of a State/Regional Agency

As background information on the variety of approaches to managing 9-1-1 within the States, the Model State 9-1-1 Plan [19] , developed by the National 911 Program Office and the National Association of State 9-1-1 Administrators (NASNA) is a good resource. It provides a succinct yet comprehensive resource to understand why each implementation of NGCS will require a thorough analysis to ensure all relevant stakeholders are considered in establishing a management and monitoring framework for NGCS.

The Model State 9-1-1 Plan conveys some of the key differences in the approaches existing across the United States. Many states have developed state-level 9-1-1 programs, though there are many differences between the nature and organizational aspects of the programs. These programs range in scope from a strong state authority that owns and operates a single statewide system that funds and provides operational support for 9-1-1, to informal or no state-level planning or coordination of any sort. Where state programs do exist, most have enabling statutes that govern and restrict 9-1-1 activities, particularly if dedicated 9-1-1 service fee oversight is involved. Most state programs engage in some form of coordination and planning. The most beneficial planning processes reflect local needs and requirements, and factor in state-level needs for the statewide functions, services, and components.

While 9-1-1 is by nature a locally based public safety service, the evolution of both wireless and Voice over Internet Protocol (VoIP) forced the 9-1-1 community to develop new institutional mechanisms to coordinate and fund the service enhancements at the state level. With the movement toward an increasingly complex world of communications, some states are beginning to explore different funding and governance models to support 9-1-1 and in migration to NG9-1-1. These governance models vary from operational control to full control of design, procurement, implementation, and operation of NG9-1-1 services and technology.

2.6.3 Stakeholder Coordinating and Reporting Structures for 9-1-1

For any region to improve 9-1-1 interoperability and functionality, collaboration and participation of relevant public safety stakeholders is essential. A formalized policy structure that provides a unified approach across multiple jurisdictions and disciplines can aid the funding, effectiveness, and overall support for communications interoperability. Establishing an oversight or administrative policy body is crucial to successfully addressing the key challenges of achieving effective communications. A policy or administrative body also provides the framework in which stakeholders can collaborate and make decisions that reflect their common objective. General guidance and recommendations for establishing interoperability and improved collaboration can be found in the publications and resources established by the DHS SAFECOM office [20]

The structure and placement of the policy or administrative body described above will vary per state and local requirements. There is not a one-size-fits-all approach that is recommended. Funding models may affect the management of NG9-1-1 and should be considered during the planning phase. Some administrative bodies that exist today for NG9-1-1, or are being considered for adoption, are summarized below. This discussion is not intended to be a full treatment of this very important aspect of how NGCS and ESInets are to be managed administratively.

SLAs should to be developed between inter-dependent or subordinate stakeholders to ensure that each knows its roles and responsibilities for reporting, cooperation, failover operations, troubleshooting, and correcting problems. Regular communication of stakeholder plans, needs, and agreed-upon service level objectives is critical to the success of an NG9-1-1 project. More complex governance structures may require additional planning and consideration of responsibilities for operating, managing, and monitoring the NG9-1-1 system.

The stakeholders for an NGCS or ESInet can vary according to governance structure. A list of common stakeholders might include:

- NGCS Manager (Vendor or Authority personnel)
- NGCS Managing Authority (Manages the NGCS Manager)

- ESInet Administrators at all levels
- Administrators of other networks connected to the ESInet
- Security Operations Management
- those that manage Transitional Systems, Services and Applications
- E9-1-1 Authority Managers dependent upon NG9-1-1 services
- Configuration Control and Change Managers
- Regulatory Agencies (FCC, DHS, PSC/PUC)
- Originating Service Providers (OSPs)
- Emergency Management Organizations (FEMA, State EMA)
- Private Emergency Answering Points (Tribal police, military, College campus, Port Authority)
- Public Information Officer (PIO)
- Service Impairment Incident Coordinator
- PSAP Managers/Supervisors and Call Takers/Dispatchers
- Application and Equipment Vendors
- External Supporting Entities (Alarm companies, Telematics Service Providers, Tow truck and Ambulance companies, hospitals, etc.)
- the Public

Note that the services and infrastructure of interest to these stakeholders can vary greatly. This document mentions stakeholder groups where the topic is of significant interest to them.

2.6.3.1 Statewide or Provincial Authority

Some states and provinces have territory-wide authority to implement and manage 9-1-1 services with the responsibility of developing all necessary system elements, standards, and cost estimates necessary to provide for the installation and operation of a statewide system.

Many times, a contractor is responsible for all system elements including hosted PSAP Functional Elements, NGCS and the ESInet. Sometimes the State or Province contracts with a vendor for territory-wide ESInet services and with different vendors for other Functional Elements. In any case, contractors should be responsible for 24 x 7 maintenance and monitoring of their system, including fault management, and notifications of service impairment or outage.

Contractors typically provide monthly operational and management reports to the 9-1-1 Authority to provide information and data concerning the usage of the ESInet and the NG9-1-1 services, to identify trends present and/or potential future problems, as well as reporting any maintenance and security related activities. The reports also demonstrate contractor compliance with the performance levels within service level agreements. In addition, the contractor may provide the 9-1-1 Authority with a management information system and other reporting and system monitoring tools. The contractor may also provide access to the raw data.

Procurement, contracting, implementation, and vendor management may be handled by the 9-1-1 Authority or another designee as appropriate. The 9-1-1 Authority staff may include a director, a technical support manager, database staff, a training manager, and GIS staff who are responsible for maintaining the GIS data and services necessary for Next Generation services, including the daily provisioning of changes to the NG9-1-1 Services Provider reported to them by municipalities.

2.6.3.2 Statewide Authority with Regional Coordination – Multiple 9-1-1 Authority Types

There are instances where a multi-regional coordination structure exists. At the State level, it provides guidelines and policies that regional 9-1-1 Authorities may apply. Regional 9-1-1 Authorities will dictate how the State serves the jurisdiction. Examples of Regional 9-1-1 Authorities include a Regional Planning Council, Emergency Communications District, or Municipal Emergency Communications District. Each is unique in how they represent the population, geography, size, funding mechanisms, and governance. Statewide coordinators are tasked to do planning and coordinate with the agencies to ensure collaboration among all 9-1-1 Authorities. This may include tasks such as the development of a strategic plan for statewide 9-1-1 service and published material about its NG9-1-1 master plan to guide the state-level transition to NG9-1-1 technology from various legacy systems.

To bring a "single voice" to the governance structure of this diverse group of 9-1-1 Authorities, statewide coordination may develop some form of an Emergency Communications Advisory Committee for the purpose of collaboration and planning the transition to NG9-1-1 in the state. Membership would include representatives from each 9-1-1 Authority type.

2.6.3.3 Multi-Jurisdictional Regional Coordination

Some implementations of NG9-1-1 that share resources in areas that cross jurisdictional boundaries (federal, state, tribal, etc.) might involve a less formal regional structure that is comprised of representatives from each jurisdiction (or sub-region) that represent the PSAPs, GIS, IT and other technical and policy disciplines within that jurisdiction. The collection of sub-regions would report into an existing legal cooperative entity, such as a

regional Council of Governments (COG) structure, through a coordinating NG9-1-1 Committee. The NG9-1-1 Committee would develop mutually supportive NG9-1-1 policies and procedures. Sub-regions or jurisdictions would maintain relationships with their state statutory structure to receive funding through existing regulatory or administrative bodies that collect 9-1-1 fees.

2.6.4 Monitoring and Managing Hardware and Software Changes

Managing change in any system of interdependent elements is inherently complex. The complexity is multiplied when elements have been provided by different vendors. A change in one vendor's system or service can adversely affect another vendor's system or service, potentially affecting the overall 9-1-1 service itself. The 9-1-1 Authority should ensure that a well-documented process is used to monitor and manage change in any system within the 9-1-1 Authority's control. Defining the process in SLAs with the participating vendor(s) is recommended. The appropriate process for managing change can vary depending on system type and governance structure, but effective change management typically incorporates the following elements in some way:

- Communications Structure – this would be a change management board or other governing body that has a representative from each stakeholder. Periodic, scheduled meetings are used to discuss any need to modify a system, service, or configuration.
- Documentation Structure – there should be a standardized form that a vendor would use to request a change the vendor believes is desirable. Using a standardized document naming and numbering scheme is highly recommended. The form should include an assessment of the risk to the overall system or individual elements.
- Test Structure – a means of testing a proposed change with other systems or services that could be affected by the change can be critical. A test lab is desirable, but many types of changes can be tested remotely between vendors. In the case of an individual PSAP, remote testing may be an effective method.
- Approval Structure - the change management board would decide collectively if and when to make the proposed change. Stakeholders need the ability to object to a proposed change, request further testing, or to propose special testing or implementation processes when needed.
- Implementation Structure – when a change has been approved for deployment in the production environment, details of when and how the change will be made are decided by the change management board with buy-in from all stakeholders.
    - It is generally recommended that only one change be deployed at a time.
    - Stakeholder Organization – must provide support and participation in the deployment and testing process.

- Validation – there should be a written test process to ensure that the change had the desired effect and did not have undesired effects. The implementation process should address backup and rollback plans if the validation test is not successful.

2.6.5 Equipment and Services to be Monitored

It is necessary for the 9-1-1 Authority supporting the NG9-1-1 implementation to establish an effective monitoring and management structure based on an essential set of management activities. Briefly, the essential elements of an effective monitoring and management structure may include:

- Data Collection Capabilities
  - SNMP, NETCONF, NetFlow, etc. – See Network Management Monitoring Section (2.2)
  - Application Logs – Many applications have an internal logging function.
  - LogEvents defined in the i3 Logging Service – See the Logging Service Section (2.7.18) and the LogEvent Replicator Section (2.7.19).
- Baseline Performance Measurements and Alert Thresholds – Establish what "normal" looks like for the NG9-1-1 implementation to allow historical reference point comparisons to real-time infrastructure performance. Specify alert notifications based on static thresholds and on standard deviations from historical norms.
- Management Information Systems (MIS) Reporting – Establish reports for key identified metrics and availability of flexible reporting tools that support actionable insights for troubleshooting on the fly.
- Proactive Data Analytics – Provide the capability of performance analysis to allow correlation of disparate data sources and time series data to move from reactive trouble shooting to proactive analysis.
- Dissemination of Alerts – Ensure that alert data is made available to all appropriate levels of interested stakeholders.

NG9-1-1 systems and services are IP-based, and therefore share some general characteristics with other IP-based systems. Any organization responsible for managing an ESInet should take advantage of the guidance and references provided in the "Network Management Monitoring" section of this document (2.2). The "Security Monitoring and Management" section of this document (2.4) provides valuable information and references for those responsible for managing security for NG9-1-1 facilities, infrastructure, applications, and services, and should be carefully reviewed and considered when designing and implementing security infrastructure and programs.

2.6.6 Managing and Monitoring GIS Services

GIS services are at the heart of NG9-1-1 systems in many ways, influencing call routing and providing a means for validation of civic addresses associated with fixed caller locations, and providing assistance in managing Incident response and resources. Advice on managing the data that underlie GIS services can be found in NENA-INF-028 NENA Information Document for GIS Data Stewardship for Next Generation 9-1-1 (NG9-1-1)[21] . "The first revision of NENA-INF-028 only covers PSAP boundaries. A future revision will cover Road Centerlines and Responder boundaries. All 9-1-1 Authorities should be familiar with the principles and best practices outlined in this document, whether the 9-1-1 Authority actively participates in managing GIS data or not. Managing a vendor that is responsible for GIS data management requires a common understanding of how the management processes work. This understanding will help the 9-1-1 Authority when defining an SLA that governs the relationship with the GIS data vendor. In addition, 9-1-1 Authorities that take an active role in managing GIS services or data should ensure that all processes result in conformance with NENA-STA-006 NENA Standard for NG9-1-1 GIS Data Model [22] .

In the NGCS, the Emergency Call Routing Function (ECRF) is the primary location-based routing element. In contrast, the Location Validation Function (LVF) is the primary mechanism to determine that a civic address location is valid for call routing and emergency response. ECRFs and LVFs are provisioned with GIS data. As a result, 9-1-1 Authorities will be required to manage and maintain GIS databases for 9-1-1 that meet new benchmarks for uniformity, data accuracy, and timeliness. These GIS databases will be the primary authoritative source for location-based call routing and location validation information. The 9-1-1 Authority should actively manage and monitor GIS services, or manage and monitor the vendor that manages GIS services on the authority's behalf.

The GIS is used to populate the LVF and ECRF databases that provide routing and validation for locations used for emergency calls. All 9-1-1 Authorities experience change in their GIS. When updates to authoritative GIS data are made, such as adding streets, changing boundaries, etc., the changes are sent to the LVF and the ECRF server via a Spatial Interface (SI). The SI is defined in NENA-STA-010 [2] . Information on managing and monitoring the ECRF and LVF functions are located in NENA-STA-005, NENA Standards for the Provisioning and Maintenance of GIS data to ECRF and LVFs [23]

For the purposes of monitoring changes to GIS data used to support emergency services, the SI operator must have a process to support sending and receiving discrepancy reports, and mechanisms to support error resolution. Changes to the GIS data should be monitored by the 9-1-1 Authority regardless of whether they choose to operate their own SIs or utilize SI services provided by an SI operator. The monitoring may be via high-level reporting by

a vendor that is managing the data, or via a very detailed change management process if the 9-1-1 Authority is managing the data.

The level of reporting from a vendor should be spelled out in an SLA and should be of sufficient detail that the 9-1-1 Authority will understand the changes or proposed changes, effective times, and anticipated impact of the changes on any affected agencies or services. GIS layers used by the LVF and ECRF to make decisions about responses to queries include civic location layers, service boundary layers, and PSAP boundary layers. Changes to these layers can have a direct and immediate impact on delivery of emergency services, and notification procedures should be carefully spelled out in the SLA or process documentation that covers GIS monitoring and management.

Metadata associated with GIS data layers is a best practice. As defined in NENA-STA-006 [22] , "Metadata is a file of information that captures the basic characteristics of the data and information resource. It represents *who, what, when, where, why* and *how* of the resource...". A 9-1-1 Authority that manages GIS data or that manages a provider of GIS data should maintain a copy of metadata files for all GIS layers that affect it. Any SLA that covers GIS data management should require updates to the 9-1-1 Authority when the metadata is changed. The metadata provided should be of sufficient detail to meet the 9-1-1 Authority's needs as described in NENA-INF-028 [21] .

Data standards for GIS are outside the scope of this document; however, there are special considerations when managing GIS data that share a boundary with other agencies. Service boundaries that define agency areas of responsibility are interdependent with neighboring boundaries, which may be defined in a GIS dataset managed by another 9-1-1 Authority or vendor. This creates interdependency between managing entities and requires cooperation in checking for and reporting of any gaps or overlaps between the boundaries. Developing an agreement with the other managing entity that governs changes to the data is important. An agreement that is essentially an SLA between the managing entities would define the activities that are interdependent, what gets reported routinely, how discovered problems are reported, and how the entities work together to resolve problems. NENA-INF-028 [21] provides significant detail on the kinds of data that create interdependencies and should be used to guide discussions of any such agreement.

In terms of GIS data and system management the 9-1-1 Authority is responsible for:

- communicating changes impacting other jurisdictions, and ensuring changes are within limits allowed by inter local or other agreements;
- coordinating and facilitating routine GIS data changes and discrepancy resolution, including between neighboring jurisdictions, or executing the changes itself if the 9-1-1 Authority maintains the data; and

- setting, reviewing, and refining requirements for participating entities to provision GIS data into ECRF and LVFs.

2.6.6.1 Mapping Data Service (MDS)

NENA-STA-010 [2] states that when answering calls out of area, the answering PSAP needs to be able to display an appropriate map covering the area in which the caller is located. NENA-STA-010 [2] defines the MDS for this purpose to provide such a map. An MDS may be provided in the ESInet and shared by multiple PSAPs. If the MDS is provided by the NGCS provider, then the NGCS provider should monitor the availability of the underlying GIS data and of the web services provided by the MDS. For example, sending frequent test requests to the MDS can provide early notification of degradations or failure. Ideally, an agency would want to test its own MDS and the MDS of neighboring agencies.

2.6.7 Management Information Systems (MIS)

Monitoring of all aspects of call processing, from call delivery to call and incident handling, is essential at every level in an NG9-1-1 operation. NENA-STA-019, NENA's NG9-1-1 Call Processing Metrics Standard [24] provides standardized measurement primitives for use by MIS and other systems for monitoring, reporting, and analysis functionality, and should be used to ensure that the outputs produced by these systems are based on common input parameters. An MIS solution can provide both 9-1-1 Authorities and individual Agencies with data-driven insights that are crucial in assessing overall system performance and can provide the Agency the information needed to manage their daily operations.

Some form of MIS is strongly recommended to assess and maintain the efficiency, efficacy, and overall performance of the NG9-1-1 system. To provide meaningful, actionable insights into NG9-1-1 functionality, performance, and overall health, an MIS system should utilize, at minimum, the NG9-1-1 Logging Service defined in NENA-STA-010 [2] . This will enable the MIS to provide both historical and real-time reporting, and potentially real-time alarming as well.

In addition to the data provided by the NG9-1-1 Logging Service, an MIS will often be able to consume data from additional sources. This will enable users to monitor the performance and efficiency of all aspects of call processing from call delivery to call and incident handling. When these various data sources are aggregated, the MIS is then able to provide helpful insights into both the technical and human elements involved in public safety activities. These multi-dimensional insights are valuable to, and can be tailored to, all stakeholders in an NG9-1-1 operation, including but not limited to: Agencies, 9-1-1 Authorities, Service Providers, vendors, technicians, and even the public.

2.6.7.1 MIS Use by State, Regional, Provincial 9-1-1 Authorities

9-1-1 Authorities can benefit from MIS offerings that monitor NG9-1-1 traffic and overall NG9-1-1 system efficiency and health, as they relate to call and incident handling. An MIS solution should report on the overall health and performance of both the NG9-1-1 system as a whole and the individual services and Functional Elements that comprise the NGCS and/or serve the NG9-1-1 PSAP. In addition to historic and real-time reporting, real-time alerting is also a function that is often provided by an MIS. NG9-1-1 PSAPs will have significant detailed data about incidents within the PSAP. When such details are made available to the 9-1-1 Authority it would be possible to do statistical analysis on overall incident processing from call receipt to responder activities on-scene.

Using an MIS, 9-1-1 Authorities can leverage the information provided by the NG9-1-1 Logging Service, in conjunction with supplemental data sources, to provide actionable, data-driven insights into things such as (but not limited to):

- overall call volume, including but not limited to the number of calls entering the ESInet, the number of abandoned calls, the number of calls successfully delivered via the ESInet across a period of time;
- call routing, allowing the optimization of wireless call delivery, thereby reducing the number of transferred 9-1-1 calls, and ultimately reduce response times;
- test call volume and results;
- call media insights, including but not limited to media type (e.g., voice, video, text/MSRP, NHI calls, etc.);
- call routing, including but not limited to initial routes provided, policy rules invoked (such as for policy-based call diversion), PSAP responses, and more;
- discrepancy reporting;
- Functional Element (FE) states, including but not limited to Element State, Service State, Security Posture, and more;
- Functional Element transactions, including but not limited to transaction types (LoST and HELD location queries, etc.), transaction volume (by type), transaction speeds (by type), and more;
- ESRP queue and dequeue transactions;
- bridging and conference details;
- PSAP status, including but not limited to Security Posture, Call Diversion Requests/Acceptance, etc.; and
- Incident or Responder driven statistics.

2.6.8 NG9-1-1 Core Services (NGCS)

The NGCS consist of multiple Functional Elements as defined in NENA-STA-010 [2] . NGCS Functional elements (FEs) can report their State to subscribers through a SUBSCRIBE/NOTIFY package such as Element State, Service State, Queue State, and Security Posture (See these sections in NENA-STA-010 [2]). In addition, servers and operating systems can report some state information. These capabilities can be used to provide alerts for a change in state, failures, and reoccurring events. See the Alert Conditions section of this document (2.1) for more details.

2.6.8.1 The Logging Service

NENA-STA-010 [2] defines a Logging Service that performs event logging and media logging for the NG9-1-1 FEs and Services. Logging Services are implemented with redundancy so there is no single point of failure, and all Logging Services should be monitored for availability by those stakeholders that depend on the Logging Services. For monitoring, the NG9-1-1 keep alive function (SIP OPTIONS) can be used to determine if the Logging Service is available. Service State and Element State can be used to determine the current State of the Logging Service (Normal, Going Down, etc.). Security Posture can be used to determine current security state of the Logging Service (Normal, Under Attack, etc.). These State notifications are defined in NENA-STA-010 [2] .

NGCS FEs log all significant steps in call processing, plus all database queries involved and all SIP requests sent or received. These "LogEvents" are defined in NENA-STA-010 [2] . LogEvents are timestamped with the time the event occurred and can be monitored in real time to analyze how the NGCS and its FEs are performing.

2.6.8.2 Call Processing Metrics

NG9-1-1 Call Processing Metrics can be computed by examining LogEvents that are generated during the processing of calls. A definitive set of metrics for Call Processing have been developed and published in NENA-STA-019 [24] . This document defines the metrics used when computing call processing statistics. These metrics are useful for MIS reporting, but many are also useful for critical real-time monitoring of the NGCS processes. For example, if the average time to process a LoST query is typically 60ms, and it suddenly goes to more than 6000ms, an administrator would probably want to look at why that was occurring. Automated monitoring software could be used to raise an alert when anomalies in the duration of call processing steps exceed thresholds.

Most of these metrics are based on LogEvents that are logged by the NGCS elements. Careful consideration should be given to how long NGCS LogEvents must be retained for reporting purposes. For example, there may be yearly statistical reports that would require retention for more than a year. The NGCS Administrator should determine the needed retention period and size the storage appropriately, as well as design any longer-term

storage process required to support this function. Note that there may be legal policy requirements for retaining LogEvent records that exceed those required for monitoring, troubleshooting, or reporting.

The following metrics, based on LogEvents, should be monitored in real-time for anomalies that might indicate a problem in the NG9-1-1 system:

- Time from when a call hits the first element in the NGCS, and when the ESRP has determined the route, i.e. where to send the call next.
- Time from when a call hits the first element in the first ESInet, and when the Terminating ESRP has determined the PSAP to which the call will be delivered. Note that this will sometimes require monitoring multiple NGCS systems.
- Time to receive a response from a query issued to any NG9-1-1 database. Examples would be LoST, ALI, Additional Data and HELD location queries. In addition, SIP Presence NOTIFY event timing can be monitored for adherence to subscription parameters. Another example would be LoST query response times that consistently exceed the requested LoST responseTime parameters (an element the query requests).
- Time between a call being sent to a PSAP and the call being answered, answer timeouts, or abandoned call.
- All call treatment failures of unknown or unforeseen nature.
- Ringtime exceeds a threshold for a PSAP.
- Dropped calls exceed a threshold for a PSAP.
- Call enters ESInet but was not delivered to a PSAP.
- Call is answered but no media can be established.
- Too many calls are being answered by the Interactive Media Response system, triggering a notification.
- Calls exceed duration thresholds.
- Hold or Park intervals exceed thresholds.
- Call time in queue exceeds threshold for that queue.

It should be noted that some of these metrics can be affected by caching on the server, causing some responses to be instantaneous. The monitoring systems should be aware of caching, and of the fact that they will probably not know for certain whether a particular response was returned from cache. The monitoring systems should take caching into

account when determining what they consider to be the "normal" processing time, and in determining what constitutes an abnormal processing time.

2.6.8.3 Additional Monitoring of NGCS Infrastructure

Additional events or items that should be monitored, more fully described in NENA-STA-010 [2] , include:

- Simple Network Management Protocol (SNMP) monitoring points and traps (see Section (2.2) on Network Management Monitoring for additional details).
- Monitoring KeepAliveFailure LogEvents. The NGCS uses a SIP OPTIONS message as a keep-alive mechanism. This event is logged if an FE gets an error or a timeout to its OPTIONS request.
- Discrepancy Reports. Errors and discrepancies may occur in any set of data, including databases, configurations, etc. The Discrepancy Report function allows any entity to notify agencies and services when any discrepancy is found. The Discrepancy Report function is intended to be generated by any entity that is using the data and finds a problem. Discrepancy Reports are not intended to be an alarm function requiring immediate response. Since all discrepancy reports must be logged, monitoring of the DiscrepancyReport LogEvents would provide information in a near-real-time fashion.
- An abnormal number of Calls Routed per a Policy Routing Rule (e.g., all call takers busy in PSAP A route calls to PSAP B). PSAP B would be interested when this situation is developing. PSAP B will know when a call arrives that has been diverted, but an NGCS manager would want to monitor and notify stakeholders when these situations are developing. Route LogEvents should be monitored to detect call diversion.
- Streaming media quality parameters that deviate from predetermined thresholds.[1] The EndMedia LogEvent, logged when the call ends, includes the "SessionReport" element from RFC 6035 [48] , which gives media quality statistics compiled during the call. The BCF typically provides real-time media quality statistics for calls in progress. These real-time statistics give a detailed view of overall media quality.
- Call Suspicion Marking (by the BCF). A call suspicion header gets inserted into the SIP INVITE when the BCF suspects the call is an attack of some sort. When the threshold for the number of calls that are marked as suspicious is exceeded, then

[1] Textual and other non-human-initiated data quality issues may be detectable only by the applications receiving and rendering the data.

notifications are made as appropriate. Downstream FEs may modify their behavior when a BCF assigns a NENA-CallSuspicion score that exceeds the downstream FEs' predetermined thresholds.

- Denial of Service (DoS) attack detection and defense by the BCF. The BCF is designed to detect request patterns that might indicate a DoS attack and to take appropriate steps to protect the NGCS (e.g., quarantine a call by moving it into an isolated area such as a Demilitarized Zone for further investigation). Protections against DoS attacks take various forms such as Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS). Such systems are deployed in various ways such as inline (can take automatic reactions) or offline (security engineers review and approve responses before they are invoked).
- NENA-STA-010 [2] defines four event notification mechanisms designed to keep interested entities informed of important changes to the state of NGCS elements and services. The SIP "SUBSCRIBE/NOTIFY" protocol is used for these notifications. Monitoring systems that support SIP should subscribe to these events. Since all state change notifications are logged, monitoring systems that do not support SIP can monitor the LogEvents to get the event information. See NENA-STA-010 [2] for details on using the LogEvent Replicator to monitor LogEvents, and for details on the four event notification packages:
    - Security Posture – notifies subscribers of a change in the security state of an FE Service. A "Green" state is the normal state. Yellow, Orange, and Red states represent progressively more serious security postures.
    - Element State – notifies subscribers of a change in the state of an FE. States include Normal, ScheduledMaintenance, ServiceDisruption, Overloaded, GoingDown, and Down. If an FE cannot be contacted, its state may be shown as "Unreachable".
    - Service State – notifies subscribers of a change in the state of a PSAP or other Service. Service States include Normal, Unmanned, ScheduledMaintenance (down), ScheduledMaintenance (available), MajorIncidentInProgress, PartialService, Overloaded, GoingDown, and Down. If a Service cannot be contacted, its state may be shown as "Unreachable". Note that one or more elements may implement a Service. Each element would have its own Element State; the Service would have an independent Service State.
    - Queue State – notifies subscribers of a change in the state of a call Queue. States include Active, Inactive, Disabled, Full, and Standby.

- Calls in Queue on the ESRPs' ingress queues. This can be monitored by subscribing to the QueueState of the ESRPs' ingress and egress queues.
- Time Accuracy. Any device deviation from standard time is detrimental to proper operation of FEs in NGCS. Deviation may result from misconfiguration, inability to connect to a standard time source, hardware clock drift, etc. NTP time source availability should be monitored. See the Time Server section of NENA-STA-010 [2] for additional information. System events about unavailability of the time synchronization source should be monitored. While there is no standard interface for monitoring these events, all operating systems do report the events.
- Domain Name System (DNS) – The NGCS or ESInet administrator will monitor and host the DNS servers as a network element. DNS servers are often located in highly redundant geo-diverse data centers and integrated in an active hierarchy directory. Monitoring changes on these DNS servers is important (e.g., checking the service to monitor if a DNS change made is unauthorized). DNS servers could reside at multiple levels and monitoring would be done at each appropriate level. See the DNS section of NENA-STA-010 [2] for additional information.
- Dynamic Host Configuration Protocol (DHCP) – DHCP must be implemented in all network elements per NENA-STA-010 [2] . The NGCS or ESInet administrator will monitor and host the DHCP servers. DHCP and DNS are part of the i3 architecture. See the Emergency Services IP Networks section of NENA-STA-010 [2] for additional information.
- Authentication servers should be monitored by the NGCS or the ESInet administrator to ensure only properly authorized users can access NGCS FEs. See the Authentication section of NENA-STA-010 [2] for additional information. Events generated by changes to user login records should be monitored on a continuous basis.

2.6.9 NG9-1-1 Collaboration Interfaces

Monitoring the status of 9-1-1 incidents and exchanging critical situational awareness data with external law enforcement agencies and homeland security partners is a sought-after capability with NG9-1-1. The more traditional collaboration methods (e.g., NCIC, NLETS, Suspicious Activity Reports (SAR) [25] and National Information Exchange Model (NIEM)) will continue to evolve technically and operationally and might be enhanced with interfaces to NG9-1-1. In parallel, the FEs contained in the NGCS in terms of databases and methods of collaboration through Emergency Incident Data Object (EIDOs), Incident Data Exchange (IDX) FEs, the Logging Service FE, and others, provide new opportunities to enhance collaboration and situational awareness reporting. Collaboration that takes place manually today through various means, including email and distributing written documents

containing summaries of incidents or trends, has the potential of becoming more automated, using direct interfaces to NGCS data sources and data analytics software. With a more continuous monitoring of data using analytics capabilities and replicated data made available from NGCS, the identification of trends might be quicker. This would allow the distribution of situational awareness reports and appropriate warnings in a much faster automated method to subscribing jurisdictions.

The 9-1-1 Authority for a state, region, or provincial implementation of NGCS should consider providing access to data to state and local Fusion Centers, Emergency Operation Centers (EOCs), FEMA partners and other Law Enforcement agencies to maximize efforts to provide for the public welfare. Often found in major urban areas, fusion centers serve as primary focal points for the receipt, analysis, gathering, and sharing of threat-related information among federal, state, local, tribal, and territorial partners. Non-standard interfaces providing such collaboration data exist today.

NENA plans to define a Collaboration FE that will support sharing this collaboration data through standard interfaces. Using Logging Services information defined in NENA-STA-010 [2] and subscribing to EIDO updates through Incident Data Exchange (IDX) FEs or other NG9-1-1 FEs could provide significant metadata for analysis by Law Enforcement or other agencies in support of specific events or incidents. Collaborators could subscribe to new or ongoing incidents based on certain filters and provide more near real-time situational awareness updates to their partner agencies. Additional information can be found in NENA's NG9-1-1 PSAP Standard, NENA-STA-023 (forthcoming) [26] .

2.6.10 External Dependencies

Managing and monitoring NGCS is dependent on a variety of external entities and other i3 systems described below.

2.6.10.1 Originating Service Provider (OSP)

The test call interface specified in NENA-STA-010 [2] should be used to verify the health of OSP connectivity and functionality on a regular basis [2] . See the Test Call section of NENA-STA-010 for further information and the Test Call Interface in Section 2.7.6 for background information on the features and functions anticipated for this interface.

2.6.10.2 Federal Communications Commission (FCC)

The Federal Communications Commission (FCC) has several requirements about monitoring and managing systems related to the provision of 9-1-1 services that should be considered in implementing monitoring and managing systems for NG9-1-1:

- The FCC requires communications providers, including wireline, wireless, Interconnected Voice Over Internet Protocol Service Providers, Broadband Internet Service Providers, paging, cable, satellite and Signaling System 7 service providers

to electronically report to the FCC and the PSAP, or other 9-1-1 Authority, information about significant disruptions to their communications systems that meet specified thresholds set forth in Part 4 of the FCC's rules [27] . The definition of the metrics used for general outage reporting are found in §4.7 and the Outage reporting threshold criteria are found in §4.9 of 47 C.F.R.. Communications providers must also report information regarding communications disruptions affecting Enhanced 9-1-1 facilities that meet the thresholds set forth in Part 4 of the FCC's rules. PSAP and NGCS administrators must ensure their contact information on file with the service provider is current to receive outage notifications.

- Notification by "Covered 9-1-1 Service Providers"[2] shall provide all useful information in mitigating the effects of the outage as well as a name, telephone number and email address at which the service provider can be reached for follow up. See footnote.
- The Covered 9-1-1 Service Provider shall provide additional information as it becomes available but no later than two hours after the initial contact.
- The notification shall include the nature of the outage, the best-known cause, the geographic scope of the outage, estimated time for repairs and any other information useful to the management of the 9-1-1 facility.
- Notifications shall be transmitted by telephone and in writing via electronic means in the absence of another method mutually agreed to in advance by both parties.
- The FCC also has specific requirements for ensuring the resilience, redundancy and reliability of communications systems, particularly 9-1-1 and E9-1-1 networks and/or

[2] Covered 9-1-1 Service Provider is defined as any entity that provides 9-1-1, E9-1-1, or NG9-1-1 capabilities such as call routing, ALI, ANI, or the functional equivalent of those capabilities, directly to a PSAP, statewide default answering point, or appropriate local emergency authority, or that operates one or more central offices that directly serve a PSAP. For purposes of these rules, a central office "directly serves a PSAP" if it (1) hosts a selective router or ALI/ANI database, (2) provides functionally equivalent NG9-1-1 capabilities, or (3) is the last service-provider facility through which a 9-1-1 trunk or administrative line passes before connecting to a PSAP. This definition encompasses entities that provide capabilities to route 9-1-1 calls and associated data such as ALI and ANI to the appropriate PSAP, but not entities that merely provide the capability for customers to originate 9-1-1 calls.

systems. A complete treatment of the requirements can be found in Title 47 of the Code of Federal Regulations, Part 12 – Resiliency, Redundancy and Reliability of Communications,Title_47_CFR_Part_12, Resiliency, Redundancy and Reliability of Communications [28] . These requirements include detailed reports and annual certifications to the FCC that the networks and systems are redundant, reliable, and resilient. These reports may not be publicly available, but a 9-1-1 Authority may discuss issues with its service provider.

- These FCC rules are expected to evolve over time and should be monitored on an ongoing basis.

2.6.11 Monitoring during the Transitional State from E9-1-1 to NG9-1-1

2.6.11.1 Gateways within the NGCS

Gateways provide connection between legacy facilities and NG9-1-1 facilities. As "edge" elements, gateways provide important monitoring points for NGCS Administrators. Common call processing and element health LogEvents defined in NENA-STA-010 [2] should be monitored for gateways:

- StartCall/EndCall – marks the start and end of call processing by the gateway.
- StartRecCall/EndRecCall – if the gateway is acting as a Session Recording Client (SRC), which sends media and metadata to a recorder, these events mark the start and end of the recording session.
- RecordingFailed – if the gateway is an SRC, the gateway logs the event when the gateway's attempt to establish a recording session fails.
- StartMedia/EndMedia – marks the start and end of media processing. StartMedia contains details on the media offered. EndMedia contains a "SessionReport" that gives Quality of Service (QoS) statistics on the session.
- CallSignalingMessage – each SIP signaling message is logged. These can be monitored for details when a problem is suspected.
- CallStateChange – will log call state changes (on hook, off hook, ring, etc.).
- MalformedMessage – a SIP message that is malformed is logged in this LogEvent;
- ElementStateChange – a change in the state of the gateway.
- DiscrepancyReport – the gateway is reporting that it got bad data from some upstream element.

- KeepAliveFailure – the gateway got an error or a timeout on an OPTIONS message it sent to another element. The SIP OPTIONS message is the "keep alive" mechanism used in the i3 architecture.

2.6.11.2 Legacy Network Gateway (LNG)

A Legacy Network Gateway (LNG) is a signaling and media interconnection point between callers in legacy wireline/wireless originating networks and the NGCS. In the final i3 "end state", the Originating Service Provider (OSP) will interface via SIP and no LNG will be required. In transition to NG9-1-1 an LNG may be deployed within the NGCS to connect it to an OSP's legacy facilities. All of the events in the "Gateways within the NGCS", Section 2.6.11.1, should be monitored for an LNG.

In addition, the following specialized LogEvents are defined in NENA-STA-010 [2] to facilitate monitoring of an LNG's functions:

- AdditionalDataQuery/AdditionalDataResponse – timing between a query and its response can be monitored for unusual delay.
- LocationQuery/LocationResponse – timing between a HELD query and its response can be monitored for unusual delay.
- GatewayCallEvent - used by an LNG, Legacy PSAP Gateway (LPG) or Legacy Selective Router Gateway (LSRG) to log a call entering or leaving the gateway on a legacy interface. These events can be monitored for detail when a problem is suspected.

2.6.11.3 Legacy Selective Router Gateway (LSRG)

An LSRG is a signaling and media interconnection point for calls routed between a legacy E9-1-1 system and the NGCS. It allows i3 PSAPs to receive emergency calls from legacy originating networks connected to a Selective Router (SR). It allows PSAPs connected to an SR to receive calls from originating networks connected to the ESInet and facilitates call transfer between i3 PSAPs and legacy PSAPs that are served by an E9-1-1 Selective Router. All the events in the "Gateways within the NGCS", Section 2.6.11.1, should be monitored for an LSRG.

In addition, NENA-STA-010 [2] defines the following specialized LogEvents to facilitate monitoring of an LSRG's functions:

- ALILocationQuery/ALILocationResponse – timing between a query and its response can be monitored for unusual delay.
- AdditionalDataQuery/AdditionalDataResponse – timing between a query and its response can be monitored for unusual delay.

- LocationQuery/LocationResponse – timing between a HELD query and its response can be monitored for unusual delay.
- GatewayCallEvent - used by an LNG, LPG or LSRG to log a call entering or leaving the gateway on a legacy interface. These events can be monitored for detail when a problem is suspected.

2.6.11.4 Legacy PSAP Gateway (LPG)

The LPG supports the interconnection of the NGCS with legacy PSAPs. The LPG supports legacy functions such as ALI database queries and protocol conversions from SIP to Multifrequency (MF), enhanced MF signaling, Dual-Tone Multifrequency (DTMF), Integrated Services Digital Network (ISDN), or other protocols. All the events in the "Gateways with the NGCS", Section 2.6.11.1, should be monitored for an LPG. The NGCS Authority is responsible for monitoring LogEvents on the LPG.

In addition, NENA-STA-010 [2] defines the following specialized LogEvents to facilitate monitoring of an LPG's functions:

- ALILocationQuery/ALILocationResponse – timing between a query and its response can be monitored for unusual delay.
- GatewayCallEvent - used by an LNG, LPG or LSRG to log a call entering or leaving the gateway on a legacy interface. These events can be monitored for detail when a problem is suspected.
- Hookflash – used by an LPG to log a hookflash that occurs on its legacy interface.
- LegacyDigits – used by an LPG to log a DTMF or MF digit sent or received on its legacy interface.

The LPG will typically log its events to the NGCS Logging Service. A PSAP with the appropriate monitoring capability is not excluded from monitoring the LPG events. It is recommended that the PSAPs be given access to any NGCS reporting facility that shows the status of the NG9-1-1 and legacy interfaces. Legacy PSAPs will monitor the legacy interface to the LPG including ALI data links, analog, MF, or other trunks, etc.

If some but not all functions of NGCS are implemented, then the authority and/or administrator of the NGCS should follow the guidelines in this document for those functions that conform with NG9-1-1 specifications.

2.6.12 System-wide ESInet (State, Regional, Provincial)

The ESInet consists of the network infrastructure and common applications like DNS and DHCP upon which the NGCS depend. In addition, there are servers upon which the NGCS

applications and services run. This infrastructure requires different management and monitoring activity from the NGCS.

The guidance given herein for managing ESInet infrastructure assumes the network was designed per the advice in NENA-INF-016, Emergency Services IP Network Design (ESIND) Document [3] and that appropriate as-built documentation exists. This documentation must include physical diagrams, logical diagrams, and configuration information such as IP addresses, subnets, VLANs, etc. There are several major parts of the infrastructure that must be managed, and some may not be under the direct control of the ESInet Administrator:

- WAN facilities
- LAN cabling
- Switch/Router infrastructure
- Miscellaneous network devices (Servers/Workstations, etc.)
- Common applications (DNS, DHCP)

DNS server CPU utilization should also be monitored for signs of unusual increased traffic that may indicate the beginning of a Denial of Service (DoS) attack. In addition, traffic patterns on switches and routers can be monitored for signs of DoS attacks.

The ESInet Administrator should view dependent entities like PSAPs, and other state, regional, or provincial ESInets as customers of its ESInet services. Therefore, the ESInet Administrator has a notification and reporting responsibility to these dependents, and appropriate SLAs should be negotiated.

2.6.13 Database Management

NG9-1-1 is dependent upon a number of databases that support routing and handling calls. Any of these databases that are operated by, or on behalf of, the 9-1-1 Authority should be monitored for changes that potentially could affect emergency services operations. The databases utilized will depend upon architecture choices, and whether it is an end-state NG9-1-1 system or in a transitional state. If a vendor is operating the database, the 9-1-1 Authority should receive at least summary reporting information on changes to the data. The level and extent of reporting should be detailed in an SLA.

Any errors or discrepancies in data that are encountered during call processing require the receiver of the bad data to file a Discrepancy Report, as detailed in NENA-STA-010 [2] . Therefore, any Discrepancy Reports (DRs), DR responses, or DR inquiries that are sent or received by the 9-1-1 Authority should be monitored and stored for auditing purposes. If a

vendor is operating the system, then the 9-1-1 Authority should require the vendor to provide Discrepancy Reports, or acceptable summaries of them, as detailed in an SLA.

Data replication (e.g., changes to GIS data or other data being pushed out to other instances of the database) must be monitored and managed as well for integrity purposes. Errors in data that are replicated make recovery somewhat more complex. A quality control process prior to replication is critical to ensuring database integrity. This quality control process should include:

- ensuring that the databases receiving the data are current, verified, and ready for the replication;
- reviewing and ensuring the integrity of the data about to be replicated; and
- testing of the replication on a fully functional, non-production instance of the database.

The administrator of a critical database should be required to submit a written database backup and restore plan for approval by the managing authority. The processes and procedures detailed in the plan should follow accepted industry best practices for regular backup, offsite storage, record keeping, and reporting. The backup process should include a reconciliation process that requires positive validation of the backup(s) and any instances of the data. Procedures to restore data should detail the process for both full and partial recovery of a database, and account for any interdependencies between databases. The plan should also detail procedures for regular, non-destructive testing of restore procedures. Any SLA negotiated with a service provider that manages a critical database on the 9-1-1 Authority's behalf should include a high-level description of the major components of the database backup and restore plan, and any reporting process agreed to by the parties.

Examples of critical databases and data conversion services that should be monitored if operated by, or on behalf of, the 9-1-1 Authority can include:

- GIS data provisioned to an ECRF or LVF and reporting on any gaps or overlaps found in 9-1-1 service boundaries and GIS data;
- any pre-provisioned database or service used to provide or support a routing location (e.g., MSAG Conversion Service);
- an Additional Data Repository (ADR) operated by, or on behalf of, the 9-1-1 Authority;
- Agency Locator Service - changes to the record of any agency connected to the ESInet. This service may be operated by another party. If so, the 9-1-1 Authority should still require reporting of any changes to the records of any of its agencies;

- Policy Store – changes to any policies that affect the 9-1-1 Authority or its agencies, such as Policy Routing Rules;
- Border Control Function configuration data and rules; and
- Logging Service data – loggers often keep an "audit trail" of data access that can be used to establish the "chain of custody" for logged data.

2.7 PSAPs and Responding Agencies

Establishing uniform methods of interaction, interoperability and collaboration with and between Vendors, Service Providers and the 9-1-1 Authorities/PSAPs is critical for effective system monitoring and rapid system restoration in times of impairment. As transition towards NG9-1-1 proceeds, it becomes more difficult to identify the basic operational responsibilities of 9-1-1 Service Providers that provide NGCS and other supporting functionality and those of the PSAP personnel managing systems and functions involved in call processing. Interworking between FEs and Services in interconnected ESInets and Agencies makes joint monitoring easier and more effective. Administrative cooperation between Vendors, Service Providers and the 9-1-1 Authorities/PSAPs facilitates reciprocal monitoring. Reciprocal monitoring agreements can improve monitoring by allowing agreement participants to subscribe to Element and Service States, sending discrepancy reports to agreement participants, forwarding SNMP traps to agreement participants, sharing statistics with agreement participants, etc.

An effective NG9-1-1 monitoring and management program for PSAP call processing functionality will include, at a minimum:

- asset management and system configuration and change control processes (i.e., a Configuration Management (CM) process);
- monitoring real time call processing;
- security impact analyses on proposed or actual changes to the PSAP systems and the operating environment;
- assessment of selected security controls employed within and inherited by the PSAP on systems (including controls in dynamic subsystems); and
- security status reporting to appropriate management and governance officials.

2.7.1 Monitoring and Managing Call Processing Functionality

A continuous monitoring strategy for the call processing systems in a PSAP should be developed to identify the security controls to be monitored, the frequency of such monitoring, and the approach for assessing the security controls. The developed strategy should define how changes to PSAP call processing systems and associated databases will

be monitored, how security impact analyses will be conducted, and the security status reporting requirements including recipients of the status reports. In addition to monitoring of NG9-1-1 communications, mitigation of suspicious or malicious communications is a key element in the overall function and goal of a PSAP in terms of its responsibilities in NG9-1-1 management and monitoring. Suggestions included within Section 2.7 can be configured and implemented in different ways depending on the circumstances and unique characteristics of the PSAP based on size, geography, and other operational considerations such as governance and funding models.

Monitoring of various metrics within the NG9-1-1 system for call processing should be implemented with the 9-1-1 Authority determining which metrics are most appropriate for collection and reporting. The NENA NG9-1-1 Call Processing Metrics Standard, NENA-STA-019 [24] , provides the metrics that should be available within an NG9-1-1 system. For Call Processing, the following metrics are a minimum set that should be monitored:

- Answered Call
- Attempted Call
- Diverted Call
- Abandoned Call
- Misrouted Call
- Call Network Transit
- Inter-Network Transit
- Session Duration
- Call Answered Delay
- Session Answered Delay
- Call Failed Delay
- Session Failed Delay
- Call Alerting Delay
- Session Alerting Delay
- Location Dereference Query Response Delay
- Hold Time
- Park Time
- Call queued Delay

- Total Call Duration
- Call Media Quality Metrics

The FCC's Task Force on Optimal PSAP Architecture (TFOPA) [29] prepared reports that provide guidance on several topics including advice on the optimal approach to NG9-1-1 implementation. Refer to the main TFOPA web page at the FCC for a complete list of all the reports the task force prepared [29] . Those responsible for managing and monitoring NG9-1-1 might find the NG9-1-1 Readiness Scorecard prepared by in the Supplemental Report of Working Group 2 of interest [29] . The "NG9-1-1 Readiness Scorecard" provides a PSAP Stakeholder with a more granular understanding of essential NG9-1-1 system elements and enables a PSAP to properly assess their position within an NG9-1-1 implementation continuum. This understanding will allow the PSAP to better plan transition steps to move from legacy 9-1-1 into a fully functional NG9-1-1 end state.

A PSAP should refer to the TFOPA reports and review the elements of the NG9-1-1 Readiness Scorecard as a preparatory step as monitoring and management plans and governance plans are developed for the technical, functional, and operational aspects and costs associated with their NG9-1-1 transition effort.

With the recent advent of supplemental 9-1-1 location data obtained by PSAPs outside the traditional process used by wireless carriers within 9-1-1, it is recommended that 9-1-1 Authorities review their procedures and guidance to ensure effective use of such data is always followed. The details and recommended best practices on supplemental 9-1-1 location data can be found in the "Recommended Best Practices for Supplemental 9-1-1 Location Data" prepared by iCERT, NASNA and NENA [30] .

2.7.2 Originating Service Provider (OSP) Connectivity and Infrastructure

The monitoring of voice and data networks from Originating Service Providers (OSPs) and the sharing of data from systems within and between PSAPs is of great importance. It is important to understand that monitoring in the legacy 9-1-1 environment and through any transitional NG9-1-1 environment and into end state NG9-1-1 will likely require adjustments along the transition implementation path in how management and monitoring system recommendations are implemented.

In traditional legacy environments, monitoring and management of OSP connectivity and infrastructure by the PSAP or 9-1-1 Authority can be accomplished by the legacy 9-1-1 Service Provider providing alarms on the 9-1-1 trunks between the Service Provider and the PSAP, as well as by monitoring the FCC outage reports the Service Provider is required to pass along to the PSAP. These outage notifications are subject to certain threshold levels and are sent to the FCC and the PSAP when an OSP reports on a service degradation in their connectivity to the 9-1-1 Service Provider. The PSAP is usually formally made aware of outages only when interruptions exceed FCC outage reporting requirements, resulting in

mandatory report filings and notifications by the Service Provider in accordance with FCC rules and orders (see Section 2.6.10.2). In a legacy environment, the PSAP typically has its 9-1-1 connectivity and infrastructure services (e.g., 9-1-1 CAMA trunks) provided by a Local Exchange Carrier through Time Division Multiplexing (TDM) networks in local Central Offices connected to Selective Router switches and the Public Switched Telephone Network (PSTN). The provided trunks typically include a set of SLAs with that provider, and such services are normally regulated by a set of tariffs negotiated by a public utility authority within the jurisdiction, or at a state or province level.

In a transitional or end-state NG9-1-1 environment, PSAP Authorities will have different network connectivity between the PSAP and the service provider networks that interface with the OSP than what exists in the legacy environment. One such example of a difference is that IP networks will exist where TDM telephony networks formerly existed and TDM telephony networks have historically had more regulatory oversight in terms of standards. Depending on how the 9-1-1 Authority has implemented NG9-1-1 within the jurisdiction, the PSAP might have multiple levels of internal and external providers for the IP networks (ESInets) that comprise the NG9-1-1 connectivity back to the NGCS. The ESInet will be interconnected to the OSPs' networks. During a transitional phase, Legacy Network Gateways (LNGs) will be used to translate TDM telephony protocols to NG9-1-1 protocols.

The PSAP's network is often a local jurisdiction responsibility (handled by an agency or department within an IT function). The PSAP may also rely on a vendor for certain PSAP network elements (routers and firewalls) within the network with distinct demarcation points that support a geo-diverse implementation. Whatever the network architecture, SLAs should be negotiated with those that manage any networks that are interconnected to the PSAP network.

If any of the PSAP applications are hosted in external networks, then SLAs are required for the network management and with and between the managers of other applications that are dependent upon the externally hosted application. The variety of environments found in NG9-1-1 point to a need for careful consideration of management and monitoring approaches, including SLAs and reporting relationships.

The network changes NG9-1-1 engenders in the PSAP environment, outlined above, require focused management attention on the SLAs a PSAP establishes with each provider involved in the NG9-1-1 service chain for call processing functionality. Including sufficient and detailed SLAs are fundamental to the PSAP's ability to hold internal and external providers to account and to ensuring an adequate and robust 9-1-1 service to the public. SLAs must speak to requirements at the PSAP level and at the NGCS level and should include, at a minimum, the following considerations:

- System Capacities and Performance (call volume, busy-hour calls, network bandwidth)

- System Performance (Network Latency, OSP connectivity, Packet Loss, Network Traffic challenges related to prioritized delivery of multimedia, and End-of-life Support for equipment)
- Media Quality and Differentiated Services Code Point (DSCP) statistics
- Service Availability, such as that based on established Mean Time Between Failure, Mean Time to Repair, and specific Resiliency and Redundancy features, according to an agreed upon formula for calculation
- Restoration Time after Incidents of differing "Severity Levels" (see Section 2.1 Alert Conditions)
- Network Operations Center (NOC) support for incident management (monitoring for, detection of, and response time to, incidents within certain time thresholds based on severity of the incident)
- Security Operations Center (SOC) support related to intrusion detection, prevention, mitigation, and vulnerability assessment and audit
- Outage/degradation notifications and escalations
- SLA performance reporting
- Notification of a default routing, or selection of default location that is provided when actual location can't be determined

PSAP SLAs should be established for NG9-1-1 service through the NGCS and ESInet. The SLAs should require the NGCS/ESInet provider to provide the PSAP with timely information on the communications connectivity status of the OSPs that interconnect with the NGCS.

2.7.3 Network Status and Outage Notifications

For PSAP or 9-1-1 Authority owned or controlled systems, every PSAP and/or 9-1-1 Authority has the responsibility of monitoring its own systems and services to detect and respond to 9-1-1 service impairments and participate in appropriate situational awareness for such systems. It can be extremely complex to monitor and respond to impairments within individual networks, and the SLAs the PSAP includes in its management and monitoring portfolio for NG9-1-1 should seek to simplify the complexity to the extent possible so that repeatable and consistent notifications are available on a regular basis. OSPs, ESInet providers, NGCS Service Providers, 9-1-1 Authorities, and PSAPs should implement a secure information system that facilitates sharing of observed network impairment issues and the ability for individual system and service providers to notify appropriate parties at the onset of an impairment.

Because of the interconnected nature of 9-1-1 systems, a service impairment in one system is likely to create a service impairment or affect another part of the system. Effective

troubleshooting and service restoration requires communication and coordination across all entities involved. Resolution of a 9-1-1 service impairment must be effectively communicated to each stakeholder. Information sharing should include both periodic updates and final resolution (preferably with a root-cause analysis that allows all parties to learn from the impairment). Timely conveyance of system impairment resolution also allows providers who have invoked alternate service architectures to return to normal operating procedures. NG9-1-1 networks can be vulnerable to Denial of Service attacks that can cause Functional Element overload and significant service degradation that must be dealt with in different ways than traditional 9-1-1 service outages, per NENA-STA-010 [2] Section titled "Element Overload". SLAs between stakeholders should specify the mechanisms and processes for sharing information about impairments and resolutions.

When interruptions and outages of connectivity occur, the PSAP should expect the Service Provider for their NG9-1-1 services to provide outage reports updates and Root Cause Analysis reports in accordance with established FCC rules, and in accordance with any response time commitments included in the SLAs. Generally, PSAPs do not have detailed visibility into the OSP on a monitoring basis (e.g., tower availability and saturation rate) as that is proprietary information. If a PSAP has a network element or capability in the connectivity to the PSAP (e.g., a microwave link) there might be some detailed monitoring tools for the PSAP to monitor that element of their overall network status. PSAPs should take advantage of any monitoring tools available to them for any communications links upon which they depend.

SLAs should require reporting of causes and actions after restoration of service following an outage or degradation. A root cause analysis report provided to a PSAP from a Service Provider regarding an outage or interruption should, at a minimum, include the following elements[3]:

- Date/Time of the start of the service impairment
- Date/Time of service restoration
- Date/Time service disruption was detected
- associated Ticket Number(s)
- number of PSAP customers impacted, to the extent known

[3] Note that this list includes many items that go well beyond what FCC rules require Service Providers to provide to PSAPs. An SLA should acknowledge those FCC requirements, and if a PSAP can negotiate any additional reporting as suggested by this list, it would be to the PSAPs benefit.

- Actual number of calls impacted, if known
- functionality lost during the service disruption (wireline, wireless, VOIP, data, Call Routing, Location Validation, Policy Routing Rules, etc.)
- corrective action(s) (completed, and future actions, as applicable)
- cities and states where failed equipment is located, if available
- cities, counties, and states impacted, as applicable

While the NGCS or other Service Provider should be able to identify the extent of a degradation, the PSAP monitoring NG9-1-1 should also establish processes and methods to reach out to neighboring PSAPs and jurisdictions during such outages to gain the clearest picture possible of the extent of any such interruption or outage to the service. Whether by standard email messages to designated contact groups, use of emergency communication alerting systems (with email ingestion interfaces to simplify their use), voice calls, radio communications or whatever means is established, the PSAP should gain information from surrounding jurisdictions and PSAPs in terms of the nature and extent of the outage to see if other PSAPs experiencing the same issue. The PSAP should invoke the use of pre-established escalation and reporting mechanisms from their Service Provider as well as leveraging any PSAP alerting systems in place. These pre-established mechanisms should be pro-active from the Service Provider to the PSAP and include multiple methods of reaching PSAP management with situation reports and descriptions of the interruption on an immediate basis at the time of the occurrence and at periodic times as the situation is managed. To be effective, these coordination mechanisms are best maintained by periodic meetings, conference calls and test messages to ensure all relevant parties are included in emergency communications.

2.7.4 MIS Use by PSAPs

PSAP users can benefit from MIS offerings that monitor NG9-1-1 traffic, as well as overall NG9-1-1 system efficiency, as these relate to call delivery to their respective PSAP. Both historical and real-time reporting, and real-time alerting are functions that can be provided by an MIS. Using an MIS, PSAP users can leverage the information provided by the NG9-1-1 Logging Service to provide actionable insights into things such as (but not limited to):

- PSAP status, including but not limited to Security Posture, Call Diversion Requests/Acceptance, Discrepancy Reports, etc.
- overall bandwidth utilization traffic types by DSCP
- call state changes (On hold, Conference, Transfers, etc.)

- overall call volume, including but not limited to both the number of calls intended for delivery to their PSAP, and the number of calls that were actually presented to and accepted by their PSAP (diverted and default-routed calls, etc.)
- call media insights, including but not limited to media type (e.g. voice, video, text/MSRP, NHI calls, etc.)
- Agent States, availability, and performance
- Bridging and conferencing details
- PSAP status, including but not limited to Security Posture, Call Diversion, etc.
- Test call volume, and results
- Incident or Responder driven statistics

2.7.5 Cybersecurity and the PSAP

All of the provisions in the Security Monitoring and Management section of this document apply to PSAPs and NGCS systems equally. This section provides additional information for monitoring and managing NG9-1-1 PSAP Cybersecurity.

The approach a PSAP adopts for protection from a cyber-attack will vary, based on factors such as PSAP size, call volume, geography, and governance structures. Regardless of these characteristics, each PSAP will need to manage its individual approach to identify, prevent and minimize exposure to cybersecurity risks and vulnerabilities.

As defined in the "Improving the Cybersecurity Posture of NG9-1-1 Systems" blog entry [31] prepared by the Department Homeland Security (DHS), the cyber infrastructure for NG9-1-1 systems includes the IP-based networks, assets, databases, and services, as they are involved in the processing, storage, and transport of data. Specifically, an NG9-1-1 system's cyber infrastructure includes:

- assets that are part of, or interconnect with, ESInets;
- Service Provider networks and applications that interconnect with ESInets;
- Government applications and services that connect to ESInets; and
- Dispatch systems and components that connect to ESInets.

Traditionally, the term "cyber" has been applied only to information technology (IT) systems and assets, while communications infrastructure was considered separate. However, defining cyber infrastructure as including both IT and communications systems accounts for the many ways in which these systems have converged. NG9-1-1 PSAP administrators should recognize this convergence to more effectively counter risks. Risks to any component of these systems could threaten an entire NG9-1-1 system or its data, so it is important to consider systems holistically.

An effective overview provided by DHS on the cyber risk to NG9-1-1 can be found at "Cyber Risk to Next Generation 9-1-1" on the DHS Cybersecurity website [31] . Another primer on the basics can be found in the APCO International document: "An Introduction to Cybersecurity: A Guide for PSAPs" [12] . The APCO document can be used to help PSAPs develop policies and procedures and raise awareness of areas that require further consideration. Also, Chapter 3 of NIST Special Publication 800-30, "Guide for Conducting Risk Assessments" [32] , contains descriptive information on how an organization, such as a PSAP, can assess its exposure to risk. Conducting a thorough risk assessment is strongly urged for any PSAP. Similarly, the DHS provides guidance on performing cyber self-assessments under the Critical Infrastructure Cyber Community Voluntary Program [33] .

The PSAP, or assigned governance team, should also monitor alerts and notifications from the United States Computer Emergency Readiness Team and other relevant sites on a continual basis (See Section 2.4.7 Securing Data Traffic). Examples of such sites include:

- US-CERT latest threats information https://www.us-cert.gov/ncas/alerts; and
- NIST National Vulnerability Database https://nvd.nist.gov/vuln.

2.7.5.1 Security Operations Centers (SOC) and the PSAP

Most NGCS ESInet implementations will include the services of a SOC at the Service Provider level to implement Intrusion Prevention System (IPS) capabilities to examine network traffic flows to detect and prevent vulnerability exploits. Likewise, Intrusion Detection System (IDS) capabilities are also usually included in a SOC to monitor a network or systems for malicious activity or policy violations. The SOC helps monitor such unusual activity that may present a security risk in the network and to identify other potential network anomalies for immediate action and follow-up. A SOC requires an organized and skilled team to continuously monitor and improve an organization's security posture. PSAP vulnerabilities are similar to NGCS vulnerabilities and PSAPs are often connected to various other networks with differing security requirements and infrastructure, so PSAPs must implement similar IPS and IDS mechanisms. A PSAP or a group of PSAPs in a region, might determine that another layer of defense should include a shared SOC at the PSAP or regional level beyond what might exist in the ESInet (e.g., local networks that are not protected by the scope of the SLAs associated with the SOC at the ESInet level).

The TFOPA report from Working Group 1 [29] discusses the concept of the SOC at a shared level in a region and uses the term Emergency Communications Cybersecurity Center (EC3). PSAPs will need to coordinate within their region and governance structures to plan the best approach to meet the issues associated with cybersecurity threats and, from that planning effort, make plans to operationalize the procedures and processes that work within the local PSAP environment. For example, the TFOPA report from Working Group 1 states: "depending on the specific needs of the PSAPs in a region, not every EC3

may require every level of security service within the EC3. 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 to those designated EC3s.

2.7.5.2 Telephony Denial of Services Attacks (TDoS)

PSAPs should implement best practices to minimize Telephony Denial of Services (TDoS) to their Public Safety Communications Service. The perpetrators of these attacks typically launch numerous phone calls against the PSAP telephony network, tying up the system and preventing the agency from receiving legitimate emergency calls. Evolving best practices are found in the APCO document: "Telephony Denial of Services (TDoS) to Public Safety Communications Phone Service" [34] . The General Accounting Office (GAO) also provided insight into the threats to cybersecurity posed by TDoS attacks [35] .

The checklist provided in the APCO TDoS document provides recommended steps "before" a TDoS event, "during" a TDoS event, and "after" such an event. "Before a TDoS" attack activities involve planning with your Service Provider, educating employees in protecting information, and ensuring circuit design is as diverse as possible to minimize overflow between circuits in times of overload. "During a TDoS" event involves recording voice and other media traffic as much as possible, documenting all known information (e.g., start and stop time, number of calls, etc.), and retaining all system call and IP logs. "After a TDoS" event activity involves reporting and filing complaints with the appropriate authorities (e.g., FBI, local police, etc.).

The Border Control Function (BCF) defined in NENA-STA-010 [2] provides security and control for SIP sessions in the NG9-1-1 system, including detection and initial defense against SIP-based TDoS attacks. The BCF can also temporarily block incoming nuisance calls, and PSAPs should be aware of this functionality and take advantage of it when required. All SIP calls processed within the NG9-1-1 system will be routed through a BCF. A BCF supports the Security Posture notification event package like other FEs. PSAP security monitoring systems should subscribe to this high-level Security Posture event notification from the BCF as part of their overall security monitoring processes. The Session Border Controller (SBC) and firewall components of the BCF typically provide substantial internal logging and alerting functionality that should be used to monitor and detect attempted intrusions and TDoS attacks. SBC processing rules and control functions are then used to respond to and mitigate a suspected attack. The PSAP must have access to a BCF, which may be in the PSAP, or be provided in the NGCS. PSAP personnel responsible for security monitoring and management should take full advantage of the BCF's logging and alerting functionality to support the PSAP's role in overall NG9-1-1 system security. When the BCF is provided in the NGCS, an SLA between the NGCS provider and the PSAP should define

roles, responsibilities, and reporting processes that utilize the BCF's logging, alerting, and call control functionality.

PSAPs that are in transition, such as those that have IP-based Call Handling systems, but are not connected to an NGCS system, should carefully consider the need for Session Border Control. TDoS attacks happen in the legacy 9-1-1 system, typically through tying up all available legacy trunks, and thereby can prevent a PSAP from receiving valid emergency calls, even when an LNG is used to convert legacy calls to VoIP calls. If the IP-based Call Handling system can receive IP-based calls from sources other than a PSAP-controlled LNG, then Session Border Control is imperative to protect the PSAP from IP-based TDoS attacks.

2.7.5.3 Cybersecurity Framework and the PSAP

NIST formally defines cybersecurity as:

> "Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation" [36] .

To ensure the most comprehensive approach to a PSAP's security environment, the PSAP should consider using the guidance outlined in the "Framework for Improving Critical Infrastructure Cybersecurity Version 1.1" [37] prepared by NIST. Using this approach should include consideration of the previous recommendations for Cyber security made immediately above. The "Framework" was implemented by a presidential Executive Order; it calls for the development of a voluntary Cybersecurity Framework ("Framework"). The Framework should provide a "prioritized, flexible, repeatable, performance-based, and cost-effective approach to manage cybersecurity risk for those processes, information, and systems directly involved in the delivery of critical infrastructure services" [37] (p.3). The Framework provides guidance to a PSAP or other regional authority on managing cybersecurity risk.

Resource constraints at the PSAP level make implementing the Framework guidance a challenge for most PSAPs. It is strongly recommended that additional resources at the regional, state, or provincial level be sought by PSAP management to ensure that most cybersecurity recommendations are considered and implemented to ensure public safety systems are adequately protected.

Building from the NIST recommended "standards, guidelines, and practices", the Framework provides a common taxonomy and mechanism for organizations to:

- describe their current cybersecurity posture;
- describe their target state for cybersecurity;

- identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
- assess progress toward the target state; and
- communicate among internal and external stakeholders about cybersecurity risk" [37] .

2.7.5.3.1 Comprehensive Information Systems Inventory

Security categorization provides a vital step in integrating security into a PSAP's business and information technology management functions and establishes the foundation for security standardization amongst their information systems. The "TFOPA Working Group 1, Optimal Cybersecurity Approach for PSAPs, Supplemental Report" [29] , Recommendation #5, is to:

> "Encourage 9-1-1 Authorities to inventory their systems and participate in Critical Infrastructure Cyber Community Voluntary Program. As part of Executive Order (EO) 13636 [38] DHS launched the Critical Infrastructure Cyber Community or C³ (pronounced "C Cubed") Voluntary Program to assist the enhancement of critical infrastructure cybersecurity and to encourage the adoption of the NIST Cybersecurity Framework (the Framework), released in February 2014. The C³ Voluntary Program was created to help improve the resiliency of critical infrastructure's cybersecurity systems by supporting and promoting the use of the Framework."

Guidance from NIST for federal programs can establish useful measures for PSAPs to adapt for security categorization of systems (e.g., classification and inventory) as appropriate. The NIST "Volume 1: Guide for Mapping Types of Information and Information Systems to Security Categories" [39] indicates that:

> "…security categorization starts with the identification of what information supports which lines of business, as defined by the Federal Enterprise Architecture (FEA). Subsequent steps focus on the evaluation of the need for security in terms of confidentiality, integrity, and availability. The result is strong linkage between missions, information, and information systems with cost effective information security".

The guidance in the NIST Volume 1 Guide, previously referenced, as well as FIPS 199, Standards for Security Categorization of Federal Information and Information Systems [40] provide a reference framework and background information PSAPs can adapt to categorize their information systems inventory and establish the appropriate level of security controls and monitoring of their systems inventory in accordance with TFOPA recommendations. Assistance in establishing these frameworks and inventory systems might require

assistance above the individual PSAP level in terms of resources to ensure consistency in approaches across ESInet deployments. PSAPs and 9-1-1 Authorities should also be aware that a commercial market exists for cybersecurity software systems and technical assistance to assist organizations in implementing adequate control mechanisms to meet minimum security requirements outlined by NIST.

2.7.5.3.2 Cybersecurity Continuing Awareness Programs

PSAPs will need to implement awareness and ongoing training programs for all aspects of security and cyber security preparedness. The Critical Infrastructure Cyber Community (C^3) Voluntary Program [41] , from DHS' US-CERT department, engages communities to promote use of the Cybersecurity Framework at events across the country. Interested parties at the PSAP or regional level can avail themselves of the DHS events and their media resource, which contains videos, webinars, and other downloadable resources, as a means of continuing education on cybersecurity. See the US-CERT web site [42] .

Other responsibilities the PSAP will need to implement include:

- assigning an individual responsibility for the cyber security strategy;
- establishing a Disaster Recovery and COOP plan that all in the PSAP are familiar with;
- disseminating Internet usage policies that are signed and followed by PSAP employees;
- keeping data backups in case of attack;
- installing all patches on all devices as soon as the patch is available;
- employing two factor authentications whenever possible;
- creating audit logs that includes User Ids, data and time of key events, (log on and log off), networks accessed and failed attempts; and
- maintaining an accurate inventory of the systems and applications on the PSAP network.

2.7.6 Test Call

PSAPs should utilize the "Test Call Generator" interface detailed in the "Test Call" section of NENA-STA-010 [2] to verify that the call path to the PSAP through the NGCS is functioning properly. The "Test Call" section also describes a "Test Call Generator" that can be used to automate the process of placing test calls. PSAPs should consider employing an automated test call process if possible, in order to continually and systematically verify the correct operation of the various elements in the NG9-1-1 call processing system, and if there are faults, failures, or other conditions that prevent the effective delivery of emergency 9-1-1

calls, take appropriate action. Continually testing a system typically provides earlier notification of problems. Automated NG9-1-1 test calls may be supported by participating originating service providers (OSPs), PSAPs, and in some cases, providers of NGCS (Next Generation Core Services) and ESInet operators.

2.7.6.1 Features and Functions

There are desirable features in any automated NG9-1-1 Test Call mechanism. The fact that NENA-STA-010 [2] does not specify all possible uses for the Test Call interface should not preclude a 9-1-1 Authority from implementing those features and functions that would be useful to it. The following features and functions are desirable:

- coordination of automatic test call generation and reception with configurable frequency, caller location, and other call variables
- quick notification (within minutes or seconds) to PSAPs, OSPs and others of faults, failures, or other conditions that prevent the successful delivery of emergency calls to a PSAP
- ability to send test calls to a PSAP regardless of whether the SIP signaling would terminate at a Legacy PSAP Gateway, a bridge, a Call Handling FE, an Interactive Media Response (IMR) or some dedicated test call device
- stress test an NG9-1-1 call processing system to determine the system's ability to process 9-1-1 calls at high call volumes
- test Policy Routing Rules
- Any automated NG9-1-1 Test Call mechanism should employ standard protocols and data formats to allow interoperability among multiple Originating Service Providers and multiple PSAPs.

Future technology and standards may provide methods to support the following features:

- test the ability of the NG9-1-1 system to process and deliver a call-back from a PSAP to a caller's device
- enable consumers to generate limited, controlled test calls

2.7.6.2 Test Call Mechanism Functions

The Test Call Section of NENA-STA-010 [2] specifies an element called a Test Call Generator, which is a web service that provides a SendCalls function. The PSAP, or other authorized entities such as ESInet Operators and NGCS Operators, should use the Test Call Generator to execute automated tests of the NG9-1-1 system. The Test Call Generator supports variables such as location, call frequency, and discrepancy rate limit. The Test Call Generator also supports notification of test failures via the Discrepancy Report web service.

However, the Discrepancy Report mechanism may not be sufficient for notifying all stakeholders of the status of an automated Test Call process. Therefore, the test initiator should consider setting up a more robust notification system.

Ideally, a Service Provider would operate a Test Call Generator that the PSAP could utilize, and the PSAP would be able to control the frequency of test calls, the time period for the test, and the number of test calls to be made (e.g., a specific number or continuous). Ideally, Test Call Generators would provide a standardized interface for PSAPs to use for any Service Provider. These mechanisms have not been standardized in the i3 architecture but would be desirable.

2.7.7 Management Console

The Management Console defined in NENA-STA-023 (forthcoming) [26] is an FE designed to monitor services and elements the PSAP depends on. These services and elements may be in the PSAP or in the NGCS. The PSAP should use the Management Console to monitor the following for these services and elements:

- Service State
- Security Posture
- Element State, when an individual element is used by the PSAP
- Queue State
- Discrepancy Reports (including Discrepancy Reports from a Test Call generator)
- System Alarms (notifications) that are configured in the Management Console
- the ESRP's ESRPNotify event (monitored directly or through Call Handling)

The PSAP is dependent on some services and elements provided in the NGCS. The PSAP should monitor the state of any services or elements it does depend on, if it has permission. It is desirable for NGCS Providers to expose the state notifications for these services or elements to PSAPs that depend upon them. These may include, but are not limited to:

- ESRP – used to route calls to the PSAP, and to transfer calls to other PSAPs
- Policy Routing Function – provides rules for routing calls
- ECRF or LVF – used to validate addresses provided by a caller or responder
- BCF provided by the NGCS – outgoing calls go through a BCF
- Bridge (if provided) – used for conferences and attended transfers
- NGCS Logging Service – may be used for primary and/or redundant logging and recording

- Any IDX provided by the NGCS that the PSAP uses (if provided) – used to exchange EIDO with other Agencies

The Management Console is also used to manage critical PSAP state used by the NGCS. The Management Console should be used to control the following states:

- Set PSAP Service State – used to manually control PSAP Service State
- Set Queue State – sets the state of queue; controls whether diverted calls will be accepted
- Set PSAP Security Posture – used to manually control PSAP Security Posture

If a LogEvent Replicator is available for LogEvents generated in the NGCS and/or in the PSAP, the PSAP should monitor the replicated LogEvents in real time if possible. LogEvents contain a wealth of useful monitoring information about the health and status of the services and elements that are logging. These LogEvents can be used to provide real-time monitoring and status displays, and to monitor processing times for key functions along the call chain.

2.7.8 Mapping Data Service (MDS)

When answering calls out of area, the answering PSAP needs to be able to display an appropriate map covering the area in which the caller is located, just as if the call was received from an in-area caller. NENA-STA-010 [2] defines a MDS that is provisioned with GIS data from the layers that are provisioned to the serving ECRF. All PSAPs must have an MDS that covers their service area. Multiple PSAPs may share an MDS. The MDS that serves a PSAP is discoverable via the Agency Locator Service defined in NENA-STA-010 [2] . The MDS provides two interfaces that out-of-area PSAPs use to retrieve mapping data:

- a Web Feature Service, which returns a set of GIS feature layers for a given area, and
- a Web Map Service, which returns a formatted image of a given area.

While the MDS is required to support queries from remote PSAPs, a PSAP may use its own MDS to provide uniform map displays to its own applications. PSAPs that have mutual aid agreements may use the MDS to provide uniform map displays to each other. PSAPs that have mutual aid agreements should subscribe to the Service State "notifier" for each other's MDS, and a PSAP should subscribe to Service State for its own MDS. See "Mapping Data Service" in NENA-STA-010 [2] for detailed specifications for the MDS. Since the MDS is provisioned from the same GIS data as the ECRF, the same guidelines for managing and monitoring GIS data apply. See the section titled "Managing and Monitoring GIS Services" in this document (2.6.6) for details.

2.7.9 Call Handling and Interactive Media Response

An NG9-1-1 PSAP's Call Handling FE handles emergency calls routed to the PSAP from the NGCS or transferred from another PSAP. An optional Interactive Media Response (IMR) FE is like a traditional IVR (Interactive Voice Response) function, except that the IMR can handle video and text as well as voice. When used, an IMR should be considered a critical function and should be monitored similarly to Call Handling. Call Handling and IMR may be implemented separately or within a single system. The Call Handling and IMR FEs are defined in NENA's NG9-1-1 PSAP Standard, NENA-STA-023 (forthcoming) [26] .

Call Handling and IMR FEs log call-related LogEvents to the PSAP's Logging Service, along with their Element and/or Service State. In addition, the Call Handling FE logs additional non call-related LogEvents such as Agent State and PSAP Service State changes, Queue State and Security Posture. An IMR FE logs Queue State if it manages any Queues and reports its Security Posture to upstream elements and logs any Security Posture state changes to its Logging Service. See NENA-STA-010 [2] for details on LogEvents. These LogEvents should be monitored in real-time to assess the current health of the PSAP and its services. Call Transfer and Callback functionality for emergency calls is defined in NENA-STA-010 [2] . Transfer and callback actions should be monitored and tracked in real time.

See the Management Console section of this document (2.7.7) for information on using the Management Console to monitor and manage the PSAP's services and external interfaces. A LogEvent Replicator (defined in NENA-STA-010 [2]) is useful for monitoring LogEvents because it feeds copies of LogEvents to other systems in real-time. Any system that implements Call Handling and IMR FEs may also offer proprietary monitoring features that provide additional information about the state of the system(s).

2.7.10 Interface to External Switching Systems (ESS)

The administrative, non-emergency communications systems within the PSAP serve as external switching systems for telephony and other administrative communications (voice mail, email, instant messaging, etc.). The ESS equipment might be represented by a traditional PBX or other communications gateway. For NG9-1-1, the ESS might share equipment to support the overall mission of 9-1-1, and if it does share, the PSAP must establish sufficient monitoring of the ESS to ensure that processing of administrative communications does not affect the processing of emergency calls. The ESS should utilize a BCF for all communications, which may be in the PSAP or may be provided in the NGCS.

The ESS logs call-related LogEvents to its Logging Service, along with its Element and/or Service State. These LogEvents and state changes should be monitored in real-time to maintain an accurate picture of the health of the system.

2.7.11 PSAP Security Monitoring and Management

PSAP Authorities should proactively secure and provide physical facilities, personnel security, and security for assets such as networks, workstations, mobile devices, servers, and cloud services. PSAP Authorities should provide appropriate training and education for all personnel in security matters that ensure policies and procedures are understood and followed. The processes and procedures for dealing with different types of threats against PSAP assets should be documented in advance so that risks to emergency services can be effectively mitigated.

The National Institute of Standards and Technology (NIST) Special Publication 800-12, Revision 1, "An Introduction to Information Security" [43] , provides introductory guidance from NIST on the high level aspects of security and management applicable to systems. More detailed guidance for PSAPS on Information Security Continuous Monitoring (ISCM) can be found in NIST Special Publication 800-137, "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations" [44] . Security monitoring is an ongoing process that needs to assess risk tolerance and implement security controls that remain effective and provide appropriate PSAP awareness of any threats and vulnerabilities. To assess whether security monitoring is effective, PSAPs can refer to Special Publication 800-53A, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations" [45] . It is written to facilitate security control assessments and privacy control assessments conducted within an effective risk management framework. The NIST publications provide a comprehensive framework for PSAPs or other 9-1-1 Authorities to begin a security monitoring program and to add or improve the monitoring over time as budgets and technology improvements allow. NIST has published a Glossary of Key Information Security Terms for use as a reference [36] .

2.7.12 Monitoring and Managing Incident Processing

Incident Processing metrics primarily involves measuring the performance in reaching significant Incident Processing events. Individual metrics may involve events reported by multiple FEs. For example, metrics of interest might include the interval between call answer (Call Handling FE) and Incident Type assignment (Incident Record Handling FE) or between call answer and unit dispatch (Dispatch FE). The presence of the telecommunicator and the 9-1-1 caller introduces human factors into incident processing and complicates the collection of metrics.

An EIDO exchange will be associated with all significant events in Incident handling and dispatch. All significant Incident state changes are defined in and will be logged per NENA STA-023 (forthcoming) [26] . An EIDO sent to, or received from, another FE is logged in an EIDO LogEvent. In cases where there was a significant change in Incident state, but there was no need to send EIDOs because the information was communicated internally within a system, the FE that knows about the state change logs it in an

IncidentOrResourceStateChange LogEvent. These LogEvents contain a wealth of information about Incident processing and response and can be monitored in real-time in order to detect operational impairments or used for reporting and analysis of Incident processing and response for future planning. NENA-STA-010 [2] specifies a LogEvent Replicator that can send copies of LogEvents to a monitoring system.

2.7.12.1 Incident Handling

When the Incident is presented to the PSAP it is typically in the form of a voice or text call. These calls are handled by a telecommunicator. Automated calls, such as alarms and sensors, may be handled by an automated attendant which may completely bypass the telecommunicator. Incidents created by mobile unit software may also bypass the telecommunicator. NENA-STA-010 [2] specifies an Interactive Media Response (IMR) FE that provides automated attendant functionality in the NG9-1-1 architecture.

Legacy automated attendants are also used in the case of an alarm or sensor system that has a direct link to the PSAP, such as an Automated Secure Alarm Protocol (ASAP) interface [47] . The incident may automatically be assigned a type and transferred to the designated dispatching Agency without involving the telecommunicator. The automated attendant must assign an Incident Tracking Identifier. The significant events are the same as for a call answered by a telecommunicator.

2.7.12.2 Dispatch

The Dispatcher is sometimes located at a different site than the Telecommunicator who answered the call. At some sites the Telecommunicator and the Dispatcher may be at the same site or may be the same person. In the case of an incident handled by an automated attendant, the presentation of an incident to a Dispatcher may be the first point in the lifecycle of an incident that a human attendant is involved.

The dispatching agency determines and dispatches the needed responders and resources. The Dispatcher communicates with and assists the responders and handles the incident until it is cleared from the Agency.

2.7.13 Managing and Monitoring Availability and Usage of Authorized External Services

i3 PSAP Networks often must communicate with local, state, and national services over multiple non-ESInet networks that will likely have various, and possibly conflicting, security policies. For example, NCIC, State Crime Information Center services, and Department of Motor Vehicles services are typically accessed via external networks. Availability of these services are often critical to the agency's ability to handle incidents. Firewalls and other security devices that protect these connections should be monitored, and alerts should be set up for both security and traffic events that may be of particular interest.

Monitoring traffic should be done through several avenues. For the PSAP, the monitoring must be done on both a Security and a Network level via a team, automated service, or vendor supported service for both internal and external traffic. All traffic that traverses the PSAP's network should be monitored per local policy. The external services may provide application-level monitoring functions that can be used to determine the availability of the service. The agency should work with a service provider to determine the best way to monitor the availability of the service.

For sensitive external services, such as NCIC or State Crime Information Center, connections are typically handled via a dedicated router or a secure web interface. The service or data provider will provide details on connection and security requirements for the service. The PSAP is responsible for securing and monitoring the traffic that traverses the internal network. The data provider can provide details on legal requirements or special instructions for handling and storing sensitive data. PSAP managers should monitor access and usage to ensure that employees are adhering to policy and legal requirements.

2.7.14 Monitoring and Managing Responder Data Services (RDS)

The Responder Data Services Functional Element (RDS FE) is an optional FE that can be used to transfer data (including streaming media) between a PSAP and emergency responder devices. Responders may be an individual agent, identified with an Agent ID, or may be a unit, identified with a Unit ID-Common as defined in "NENA-STA-021.1-201X Emergency Incident Data Object (EIDO)" (forthcoming) (49). The RDS FE is specified in NENA STA-023 (forthcoming) [26] .

Much of the data sent to or from responder devices will be contained in an EIDO or accessed via a link provided within an EIDO. EIDOs are logged, and the EIDO LogEvents contain the data and links sent in either direction. These EIDO LogEvents can be monitored via the Logging Service as needed. Any media streamed to or from a responder device through the RDS FE can be monitored for type, status, and content. Additional Data accessed by a responder can be monitored for type and content. Responder device status should be monitored for all of the following, when provided by the RDS FE:

- Registration (connected devices)
- Location
- Device state (active, inactive, emergency alert, etc.)
- Responder or Unit associated with the device
- Remote control commands (activating, deactivating, or invoking a device function)

Responder devices typically communicate via a server, and the RDS may be incorporated in the server. Maintaining the list of allowed devices in the server will be a regular maintenance task. Alerts should be enabled, where possible, for unusual events such as

attempts to register or connect by unauthorized devices, when a responder triggers creation of a new Incident, or when a link or merge action occurs with an existing Incident.

2.7.15 Push-To-Talk (PTT) Communications Infrastructure

Technology that supports communications with responders is evolving, including new applications such as Push-To-Talk (PTT) over IP networks. Maintaining reliable PTT communications with responders and other Agency personnel is critical to any Agency's mission. These communications are dependent on applications and infrastructure that must remain functional to support reliable communications. PTT systems include traditional Land Mobile Radio (LMR) systems and newer IP-based PTT systems that operate over a variety of networks, including the FirstNet. PTT communications applications and systems provide monitoring interfaces and capabilities that provide system administrators with real-time health and status information of the system. Monitoring interfaces and capabilities vary based on the technology and configuration of system and its manufacturer, but typically provide the following functionalities:

- System status
- Site/tower status
- Controller component status
- Conventional, trunked, and IP-based PTT system status
- Microwave, optical fiber, and copper backhaul status
- Subscriber or user device status and location
- Dispatch console system device status
- Device registration status
- Alerts and notifications
- Status of interoperability links with other agencies PTT systems
- Application connectivity status (logging and recording, consoles, etc.)

2.7.15.1 Monitoring Traditional LMR PTT Systems

System administrators typically monitor and manage traditional LMR PTT communications systems using Network Management Systems (NMS), either provided by the manufacturer as part of the system purchase or by a third party. The PTT communications NMS should be hierarchical and capable of incorporating multiple management systems into a high-level management system, providing a single point to manage the functionalities of multiple subsystems previously separated. It is important that all subsystem NMS be able to send all traps, alarms, and notifications to the supplied integrated NMS, allowing system

administrators to monitor proper equipment configuration, operation, and integration of PTT communications systems. For some legacy LMR systems, having a single interface to manage all components may not be possible.

2.7.15.2 Monitoring IP-Based PTT Systems

IP-based PTT communications systems come in three primary configurations:

- The traditional LMR equipment manufacturers offer IP-based PTT capabilities integrated with private radio systems using smart phones, tablets, and other devices.
- Commercial wireless carriers offer a variety of carrier-integrated PTT capabilities, which rely on the carriers' network to provide communication capabilities, known as Push-To-Talk over Cellular (PTToC).
- Third-party manufacturers also offer Over-The-Top (OTT) PTT services and applications. OTT services are applications that use commercial wireless carrier network connections to provide users with PTT communications services via the application riding over-the-top of the network.

System administrators monitoring IP-based PTT services over private LMR networks should use the capabilities of an NMS to monitor the status and health of the PTT interface. Key metrics to monitor include availability, utilization, throughput, priority/pre-emption, and latency, which significantly impact the quality of voice communication.

Administrators monitoring their Agency's PTToC and OTT services should use management tools provided by the carrier or OTT provider when available, but typically must rely on the carrier or application vendors' performance guarantees. Often there will be an integrated toolset used to provide end-to-end monitoring and management of these services and applications. Agencies should include reporting requirements in SLAs negotiated with PTT Service Providers.

PTT system administrators should configure their systems to provide automated alerts and notifications for all potentially critical system functions, applications, and infrastructure, and should have written procedures for mitigating and recovering from any foreseeable system degradations or failures. A PTT system is also dependent upon private and public IP and/or other networks over which it communicates, so the health and status of these network paths should be continually monitored. System administrators should also coordinate closely with the vendors maintaining the private and public networks for which the PTT systems rely on to implement and manage SLAs that meet public safety reliability requirements.

NENA-STA-023 (forthcoming) [26] defines a PTT Logging Interface that implements the RFC 7866 SIPREC protocol Session Recording Client interface for recording PTT media and

associated meta-data to the Logging Service. If there is a failure to record media or metadata, the PTT system will log a RecordingFailed LogEvent. This LogEvent should be monitored along with the StartRecCall, EndRecCall, StartRecMedia, and EndRecMedia LogEvent.

2.7.16 Change Management

Changes to PSAP systems and services should follow the guidelines in Section 2.6.4 of this document titled "Monitoring and Managing Hardware and Software Changes".

2.7.17 PSAP Multimedia Feeds

NG9-1-1 increases the communication bandwidth of a PSAP due to the IP connectivity of the ESInet and promises to introduce multimedia files or feeds into the PSAP for call processing that often will be attached to, arrive with, or be separately provided from the 9-1-1 call. The type of multimedia an i3 PSAP will need to manage, monitor, and record will likely include:

- Pictures
- Wearable monitors data from 9-1-1 callers (heart rate, pulse, etc.)
- Real time text, text messaging and chat communications
- Streaming video from mobile devices at an emergency scene, or video relay services
- Vehicle telematics
- Security and traffic camera feeds (traditional CCTV video or IP camera feeds)
- First responder Body Worn Camera media (BWC)
- Streaming media from Unmanned Aerial Craft (UACs)
- Non-human-initiated calls from sensors and alarms, including Internet of Things (IoT) sensors
- Facial, biometric, object recognition, and Artificial Intelligence applications
- Social media feeds (Twitter, Facebook, etc.)
- Commercial television feeds via IP
- Automatic Vehicle Location (AVL) systems

PSAPs will have the latitude to handle the processing of such multimedia calls in the traditional manner where call takers and dispatchers handle all aspects of processing the call from an end-to-end perspective at their respective workstation. In this traditional manner, PSAPs may find that the display of such multimedia files associated with a call requires additional physical monitors or display area on existing monitors. Multimedia

technologies and delivery methods are expected to evolve and PSAPs should be prepared to evolve their monitoring capabilities as needed to manage the new media technologies.

Some PSAPs might find the need for new workstation arrangements where high-profile call situations require "dedicated resources" such as certain PSAP staff, or other public safety personnel such as police officers who are available to perform highly focused real-time reviews and analysis of video streaming from an in-process emergency scene. These "dedicated resources" and workstation and equipment arrangements could be locally based at a PSAP, off the operations floor in a dedicated space, or regionally-based when appropriate. The setup would include secure real-time links to video feeds from the PSAP where the call taker or dispatcher is engaged with a video-rich call to the "dedicated resource" room. The setup could be used when the amount of information from the streaming video requires expert or specially-trained human assistance and likely will require advanced playback tools to rapidly piece together information from the video to pass on important clues or situational awareness to responding units. Artificial Intelligence software could be included to assist in the recognition of patterns or sounds from the streaming video to assist decision makers. The staff resources do not need to be dedicated full-time to video analysis but be available for redirection from other duties for the period of time an incident requires dedicated attention. However, if an agency plans to handle these complex incident situations, the plan should include a process for management to monitor accesses to multimedia feeds and the bandwidth being consumed by them, in order to better manage the agency's needs during these times. Such monitoring may expose the need for additional bandwidth during such Incidents.

An example of a video call where a separate video analysis team might be utilized could be a streaming video from a mobile device by a witness at the scene of an "in progress" shooting incident at an outdoor recreational field. The witness is hiding from the shooter, but active firing of rounds can be heard from the witness phone which is pointed, in a shaky trembling fashion, toward the area where the perpetrator is thought to be located, while the witness provides audible descriptive information about a chaotic scene as best as they can determine from their hidden vantage point.

Such situations might require the full time and attention of the call taker in querying the voice calls inbound to the 9-1-1 center. This type of situation might introduce the need to rapidly employ the dedicated resources necessary to view multiple streams of incoming video at a different console environment, in order to sort through the confusing images, the video streams are displaying. If an agency employs such an on-demand response team for concurrent review of streaming video for a developing situation, specialized training might be required. The training to do rapid video review and analysis for clues, as well as using specialized playback software and workstations to perform the review of multiple videos files, will require staff trained in techniques and procedures to effectively manage the unfolding scene of such intense incidents. Responders in the field may find that video

can be an effective tool to help with their response. The 9-1-1 Authority must decide how video may be selectively and efficiently provided to responders over a broadband network (i.e., via a link or an automated stream).

2.7.17.1 Planning for Multimedia for NG9-1-1

Considerations to effectively prepare to manage and monitor the multimedia environment of the i3 PSAP include:

- Local 9-1-1 Authority requirements and policy
- Statutory requirements and regulations for data retention and privacy
- Physical storage and administrative capabilities to securely manage multimedia data storage farms
- Cybersecurity procedures and systems to protect all NG9-1-1 elements from malware and other intrusions potentially introduced by multimedia files (video clips and live feeds)
- Sharing of multimedia files with others, as needed, in a real-time environment for cooperative analysis by PSAP staff and other First Responders (police, fire, EMS, fusion centers, etc.)
- Secure and efficient sharing across interconnected systems (e.g., FirstNet and NG9-1-1)
- Secure video retrieval involving Police departments that utilize chain of custody procedures to protect the forensic integrity of the media. Would include keeping an audit of data access
- Specific training for competency in analyzing multimedia feeds for public safety purposes (e.g., effective observation techniques, role and use of video evidence, procedures for videoing incidents, etc.)
- Implement controls to prevent any unauthorized interception, duplication, transmission, or other diversion of multimedia

The 9-1-1 Authority should plan for these procedures, policies, and activities prior to implementing an NG9-1-1 system, or to adding video capabilities to a transitional NG9-1-1 system. The 9-1-1 Authority should also plan for monitoring multimedia usage, including video, using the same mechanisms specified in this document for all types of NG9-1-1 calls.

2.7.17.2 Situational Awareness benefits of Multimedia in the PSAP

Safety and security purposes for using multimedia in a PSAP include, but are not limited to:

- improved protection of citizen callers, the general public, and first responders by having available real-time, or near real-time visual indications, including video of the emergency scene,
- protection of key public property and buildings, including building perimeters, entrances and exits, lobbies and corridors, receiving docks, special storage areas, laboratories, etc.,
- monitoring of common areas and areas accessible to the public, including transit stops, parking lots, public streets, and pedestrian walks,
- investigations of criminal activity,
- protection against an act of terrorism or related criminal activity,
- protection of Critical Infrastructure as defined under the USA Patriot Act, or the United States Department of Homeland Security, and
- advanced machine vision functionality like person, facial, vehicle, and license plate recognition provides additional detail about the scene.

The 9-1-1 Authority should plan for the new types of media that will probably become available, and think through how the media, the bandwidth, and storage it will consume will be monitored and managed. The 9-1-1 Authority should also plan for personnel that will be required to manage and utilize the media in handling Incidents, and to produce legal records after the fact.

2.7.17.3 Privacy and Legal Considerations of Multimedia in the PSAP

There are considerable policy, privacy, confidentiality, and legal considerations around the access to or internal or external resourcing of multimedia collected from public or private spaces. The 9-1-1 Authority needs to carefully consider these issues, and probably obtain legal advice when formulating policies for the use and management of multimedia. At a minimum, the following policy issues need to be considered:

- Video and CCTV monitoring and recording are always conducted in accordance with all existing 9-1-1 Authority policies, including any Non-Discrimination Policies, Sexual Harassment Policies, and other relevant policies. Monitoring based solely on the characteristics and classifications such as race, gender, sexual orientation, national origin, disability, etc., should be carefully considered.
- Monitoring or recording restrictions on multimedia other than 9-1-1 calls need to be considered (an example would be capturing audio in a private space). Such monitoring may be a violation of law (e.g. United States Code, Title 18, Section 2511 "Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited").

- Logging and monitoring in a manner that does not violate a reasonable expectation to privacy or a law or regulation thereto.
- Cameras may be monitored in real time by PSAP staff, but cameras may also be unmonitored while recording is underway.
- Violations of the responsibilities and procedures related to video monitoring set forth by the 9-1-1 Authority may result in disciplinary action consistent with the rules and regulations governing employees of the 9-1-1 Authority.
- PSAPs must provide a copy of the logged video upon request by investigative authorities in connection with any ongoing criminal investigation, unless prohibited by law, including but not limited to the Health Insurance Portability and Accountability Act (HIPAA) and the Family Educational Rights and Privacy Act (FERPA).
- The local Information Security Office (ISO) may audit any department's video/CCTV surveillance operations for policy compliance, including recording storage and retention.
- All departments responsible for a video/CCTV monitoring system should develop and maintain written policies and processes in place to prevent camera operators tampering with, intercepting or duplicating recorded information.
- Personnel involved in monitoring and recording must be trained and supervised by their department in the responsible use of the technology and the requirements of any local policies.
- A PSAP deploying video or CCTV security systems must obtain the services of a qualified vendor to ensure the video transmissions are protected from unauthorized access or tampering in conformance with 9-1-1 Authority and other relevant technical standards.

2.7.18 The Logging Service

NENA-STA-010 [2] defines a Logging Service that performs event logging and media logging for the NGCS and for PSAPs. Logging Services are implemented with redundancy so there is no single point of failure, and all Logging Services should be monitored for availability by agencies that log to them, including the 9-1-1 Authority responsible for the NGCS and multiple PSAPs in the case where the NGCS Logging Service is shared. If a PSAP has its own logging it should monitor that logging service along with any external logging service that provides redundancy.

Monitoring a Logging Service is accomplished using standard interfaces defined in NENA-STA-010 [2] . Agency applications should subscribe to the Logging Service's Service

State to receive notifications of changes in state of the Logging Service as a whole. Element State provides notification of changes in a single Logging Service FE.

A Logging Service can consist of one or more Logging Service FEs. A single FE might report shutting down as its Element State when being rebooted, but the Service State would report "normal" if other FEs in the Logging Service continue to provide uninterrupted service. An agency should always monitor Service State and should also monitor Element State if it is responsible for individual Logging Service FEs. The PSAP Management Console described in NENA-STA-023 (forthcoming) [26] is required to monitor both Service and Element states.

In addition to Element and Service State, all NG9-1-1 FEs can be monitored using the SIP OPTIONS keep-alive mechanism as described in NENA-STA-010 [2] . FEs that log to the Logging Service should use this mechanism to monitor the Logging Service FE application's availability. Network "pings" can be used to monitor the presence of a server on the network. NENA-STA-010 [2] provides a Security Posture State "notifier" that allows services and FEs to report security state changes when under attack, including the level of any degradation being experienced as a result of the attack. The PSAP Management Console described in NENA-STA-023 (forthcoming) [26] is required to monitor Security Posture. See the Security Posture Section of NENA-STA-010 [2] for details.

9-1-1 Authorities may want to monitor who is accessing data on the Logging Service and for what purpose. A Logging Service implementation may provide a proprietary interface for monitoring accesses to its data. The NENA STA-023 (forthcoming) [26] defines a standard LogEvent that the Logging Service and other FEs use to log accesses to their data. These events can be retrieved via the Logging Service's LogEvent web service that is also used to retrieve call and Incident related events.

2.7.19 LogEvent Replicator

NENA-STA-010 [2] defines an optional LogEvent Replicator that accepts LogEvents on its input, and outputs duplicate copies of those LogEvents to two or more destination applications ("listeners"). The LogEvent Replicator makes it possible to support applications that perform system monitoring and reporting functions without requiring the FEs that are sending the LogEvents to write to the applications directly. LogEvents contain a wealth of information about how an overall NG9-1-1 system, such as how an NGCS system or a PSAP's systems are functioning.

An NGCS monitoring system could use LogEvents to watch the performance of the NGCS and raise an alarm if performance degradation is detected. A PSAP monitoring system could perform a similar function. An Agent monitoring system could use Agent State change LogEvents to monitor and report on Agent status, performance, and availability. These monitoring applications would implement the LogEvent Client interface to receive

copies of events from the LogEvent Replicator. The applications are not otherwise standardized. 9-1-1 Authorities should take advantage of any available monitoring applications offered by vendors that meet their needs.

The LogEvent Replicator will return a status code to the FE that sent a LogEvent. One of the output ports to "listeners" on the Replicator is designated as the "master" port; the Replicator will use the status code from this port as the one it returns to the FE. Status codes returned on other ports are ignored, and it is not possible for the FE that sent the LogEvent to know these other status codes. See the LogEvent Response section of NENA-STA-010 [2] for details.

The LogEvent Replicator was designed to support applications that are less critical than the Logging Service. While it is possible for a Logging Service to be one of the clients of a Replicator, doing so makes the Logging Service dependent upon the Replicator. The Replicator isn't defined as a critical element in NENA-STA-010 [2] and therefore doesn't have the same availability requirements. It is even more inadvisable to use a LogEvent Replicator as the "front end" for multiple Logging Service instances in an attempt to achieve high availability. The LogEvent Replicator is not designed for redundancy like traditional load balancers are and would instead be a single point of failure, which is not allowed for critical services in NENA-STA-010 [2] (see the Emergency Services IP Networks section of NENA-STA-010 [2]). Instead, implementations should follow the advice in the Redundancy section of NENA-STA-010 [2] and implement an active-active Logging Service architecture. In an active-active design, FEs would send LogEvents simultaneously to two or more Logging Services, or possibly to a pair of redundant load balancers that each serve multiple back-end Logging Service instances.

3 Impacts, Considerations, Abbreviations, Terms, and Definitions

3.1 Operations Impacts Summary

This Information document will likely have a considerable impact on Operations in NG9-1-1 as its purpose is to inform 9-1-1 Authorities at multiple levels of best practices and recommendations for successfully implementing NG9-1-1. These recommendations are meant to minimize negative impacts to operations when NG9-1-1 is implemented by providing the best available advice on approaches that have been successful in 9-1-1 centers or industry across a multitude of operational areas.

3.2 Technical Impacts Summary

Adopting the recommendations in this document is expected to have a significant effect on the technology utilized by 9-1-1 Authorities as they transition to an end-state NG9-1-1 architecture. NENA's i3 solution defines many mechanisms for monitoring the health and status of NG9-1-1 systems and services. Examples include LogEvents, Service and Element

State notifications, Security Posture notifications, a Test Call mechanism, and others. Utilizing these mechanisms, along with traditional network and application-level monitoring mechanisms recommended in this document will provide agencies with the data needed to manage NG9-1-1 systems and infrastructure. It is likely that the existence of the new i3 monitoring and management mechanisms will spur innovation and the creation of new tools and analysis software that utilize these new i3 mechanisms to improve monitoring and management capabilities.

3.3 Security Impacts Summary

This document has an entire section devoted to Security, Section 2.4 Security Monitoring and Management. The advice in this document is drawn from NENA standards and information documents covering security requirements as well as 9-1-1 community standards and best practices. 9-1-1 Authorities that adopt these standards and best practices should see a substantial improvement in their security posture at all levels. Failure to give adequate consideration to security issues prior to NG9-1-1 implementation can have an equally substantial negative impact on security and operations.

3.4 Recommendation for Additional Development Work

A future revision of this document will provide guidance on monitoring specific NG9-1-1 call processing metrics and on setting reasonable thresholds for triggering alerts indicating that a degradation or outage condition may exist. See NENA-STA-019 NG9-1-1 Call Processing Metrics Standard [24] for more information on the metrics.

3.5 Anticipated Timeline

Transition to NG9-1-1 can take several years and since the guidance provided in this document is applicable through all stages of transition, the anticipated timeline of the guidance will be the same as the timeline for the NG9-1-1 implementation. The implementation timeline for NG9-1-1 is likely to vary based on transition implementation and design decisions.

3.6 Cost Factors

There are costs associated with the effective Managing and Monitoring of NG9-1-1. The costs may appear in different ways depending on the approach the 9-1-1 Authority takes to implement NG9-1-1. For instance, if the approach is more along the lines of a 9-1-1 Authority entering into a service model for NG9-1-1 Core Services (NGCS) under a contract with an NG9-1-1 Service Provider, many costs might be bundled into the service offering of that provider. A 9-1-1 Authority that retains more operational and technical control of NGCS services (e.g., in-house technical staff) might need to independently establish monitoring systems and associated network connectivity to gather the data from NGCS element measuring points. In the latter case, the individual cost elements of an effective Monitoring

and Management of NG9-1-1 might be more evident since they are not provided by an outside Service Provider.

Typical costs associated with an NG9-1-1 Management and Monitoring approach may include, but are not limited to, the following:

- purchase of a commercial software monitoring system that would collect a variety of data from multiple monitoring points in the NG9-1-1 system infrastructure
- costs associated with enabling connectivity to monitor status of components (cabling, training of NOC personnel to understand the information provided by the alert, documentation to explain the alert and procedures for NOC personnel to take in reaction to various thresholds of the alarm [critical, major, minor])
- costs associated with documenting an accurate inventory and diagram of the network infrastructure and maintaining it in an automated fashion to facilitate maintenance and troubleshooting and training
- provisioning and maintenance of a Test Call Interface
- costs associated with exercising COOP plans (staff overtime, incidental supplies, transportation costs, redundant support systems, etc.)
- costs associated with securing facilities that support multiple PSAPs for NG9-1-1 (cameras, motion sensors, physical barriers) and the human resources to monitor the extra security measures put in place to support critical infrastructure facilities
- additional security awareness training and cyber security training to maintain a consistent level of awareness and ongoing compliance audits for any security audits
- training costs and associated staffing impacts on personnel to deal with new media (video, pictures, etc.)
- MDS at the PSAP (additional capability required and its impact on any existing mapping applications already in use at the PSAP)
- costs of additional infrastructure to allow increased collaboration with regional/state and federal partners for NG9-1-1 information and data
- development of an agency-specific set of performance measures and thresholds for triggering management responses to key operations events (e.g., call diversion, PSAP readiness, etc.)
- QA processes and the personnel required to perform the monitoring function
- integration and interfacing with current computer and network systems (if applicable)

- recurring costs (software licensing, maintenance agreements, hardware/software media updates)

3.7 Cost Recovery Considerations

Not applicable.

3.8 Additional Impacts (non-cost related)

The information or requirements contained in this NENA document are expected to have several impacts, based on the analysis of the authoring group. The primary impacts are expected to include:

- Significant data increase. NG9-1-1 implementations will expand the metadata for public safety information and will result in increased volumes of structured, semi-structured, and unstructured data that will be available for data mining and other advanced analytics applications. This will impact 9-1-1 Authorities in planning for and incorporating comprehensive management systems given this significant increase of data available for monitoring NG9-1-1 Functional Elements, related systems, and network elements. The amount of monitoring data available in NG9-1-1 (both structured and unstructured data) is much greater than the data gathered and monitored for traditional legacy E9-1-1 systems and networks. 9-1-1 Authorities will need to carefully consider their approach to using this additional monitoring data and its impact on business processes that collect the data in coherent, efficient systems and procedures. One key to managing this monitoring data is to make the data useable and consumable for management purposes. As additional data is gathered for NG9-1-1, careful attention is necessary to ensure that meaningful data collection and analysis is done to allow the 9-1-1 Authority to make reasoned, near real-time actionable decisions for public safety.
- Out-of-Area Call Support. With the ability of NG9-1-1 to eventually provide additional advanced information to a 9-1-1 Authority to support out-of-area call treatment and dispatch (e.g., the MDS), the monitoring and management of new Functional Elements with NG9-1-1 are likely to generate new best practices. As such best practices for out-of-area support across traditional 9-1-1 Authority boundaries are gathered, the differences for call processing support systems and NGCS functionality will likely have impacts on the training, systems, and legal requirements for 9-1-1 Authority data custodians and other 9-1-1 Authority business processes.
- NGCS to NGCS Interoperability. Monitoring the effectiveness of how separate service providers' NGCS systems interoperate is not widely done today given the low number of complete NG9-1-1 deployments. The effectiveness of disparate NGCS implementations from different service providers that frequently interoperate (e.g., across a state boundary where each state has a different service provider) has not

yet occurred enough to judge the impact. Given this current situation, the impact of true interoperability among disparate NG9-1-1 deployments is an area that will require further analysis and study from a monitoring and management standpoint, but the authoring group is certain the impact will be significant.

- The adoption of the recommendations in this document should improve the reliability and performance of NG9-1-1 systems.

3.9 Abbreviations, Terms, and Definitions

See NENA Master Glossary of 9-1-1 Terminology, NENA-ADM-000 [1] , for a complete listing of terms used in NENA documents. All abbreviations used in this document are listed below, along with any new or updated terms and definitions.

Term or Abbreviation (Expansion)	Definition / Description
9-1-1 Authority AKAs: Authority Having Jurisdiction (AHJ), 9-1-1 Governing Authority, 9-1-1 Administrator	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.
ACL (Access Control List)	A security mechanism used to allow or deny access to either computing or networking systems (e.g., access through a firewall).
ADR (Additional Data Repository)	A data storage facility for Additional Data. The ADR dereferences a URI passed in a SIP Call-Info header field or PIDF-LO <provided-by> element and returns an Additional Data object block. It replaces and deprecates the concept of CIDB previously defined in NENA-STA-010.
ALI (Automatic Location Information)	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.
ANSI (American National Standards Institute)	Entity that coordinates the development and use of voluntary consensus standards in the United States and represents the needs and views of U.S. stakeholders in standardization forums around the globe. https://www.ansi.org

Term or Abbreviation (Expansion)	Definition / Description
APCO (Association of Public Safety Communications Officials)	APCO is the world's oldest and largest not-for-profit professional organization dedicated to the enhancement of public safety communications. https://www.apcointl.org/
AVL (Automatic Vehicle Location)	A means for determining the geographic location of a vehicle and transmitting this information to a point where it can be used.
BCF (Border Control Function)	Provides a secure entry into the ESInet for emergency calls presented to the network. The BCF incorporates firewall, admission control, and may include anchoring of session and media as well as other security mechanisms to prevent deliberate or malicious attacks on PSAPs or other entities connected to the ESInet.
BWC (Body Worn Camera)	In policing equipment, a body-worn camera, is a wearable audio, video, or photographic recording system used to record events in which police officers or other law enforcers are involved.
C3 (Command, control and communications)	Command, control, and communication (c-cubed) functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission
CAMA (Centralized Automated Message Accounting)	A type of in-band analog transmission protocol that transmits telephone number via multi-frequency encoding. Originally designed for billing purposes.
CCTV (closed-circuit television)	A TV system in which signals are not publicly distributed but are monitored, primarily for surveillance and security purposes.

Term or Abbreviation (Expansion)	Definition / Description
COG (Council of Governments)	Councils of governments (also known as regional councils, regional commissions, regional planning commissions, and planning districts) are regional governing and/or coordinating bodies that exist throughout the United States. COGs are normally controlled by their member local governments, though some states have passed laws granting COGs region-wide powers over specific functions, and still other states mandate such councils.
COOP (Continuity of Operations Plan)	The ability to continue operations during and after a service impacting event through a specific set of procedures designed to reduce the damaging consequences of unexpected events resulting in the loss of 9-1-1 capabilities.
Configuration Management (CM)	Configuration management, as defined by the International Technology Infrastructure Library (ITIL), is the process responsible for maintaining information about Configuration Items required to deliver an IT service, including their relationships, to maintain its integrity over time. The information is managed throughout the lifecycle of the configuration items. Additional information can be found at: http://www.knowledgetransfer.net/dictionary/ITIL/en/Configuration_Management.htm.
Cybersecurity	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. https://csrc.nist.gov/publications/detail/nistir/7298/rev-3/final
DHCP (Dynamic Host Configuration Protocol)	A widely used configuration protocol that allows a host to acquire configuration information from a visited network and an IP address.

Term or Abbreviation (Expansion)	Definition / Description
DHS (Department of Homeland Security)	DHS is a federal agency designed to protect the United States against threats. Its wide-ranging duties include aviation security, border control, emergency response and cybersecurity.
DiffServ	A quality of service mechanism for IP networks characterized by a code in a field of a Packet called a "Code Point" and a "Per hop Behavior."
DNS (Domain Name Server)	Used in the Internet today to resolve domain names. The input to a DNS is a domain name (e.g., telcordia.com); the response is the IP address of the domain. The DNS allows people to use easy to remember text-based addresses and the DNS translates those names into routable IP addresses.
DoS (Denial of Service)	A type of cyber-attack intended to overwhelm the resources of the target and deny the ability of legitimate users of the target the normal service the target provides. DDoS (Distributed Denial of Service Attack). A distributed denial-of-service (DDoS) is where the attack source is more than one, often thousands of, unique IP addresses. A DDoS attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for example a botnet) flooding the targeted system with traffic. TDoS (Telephone Denial of Service). Illegal attacks targeting the telephone network by generating numerous 9-1-1 phone calls, tying up the network and preventing an agency from receiving legitimate calls.
DR (Discrepancy Report)	A discrepancy report (DR) function exists in NG9-1-1 to notify agencies and services (including the BCF, ESRP, ECRF, Policy Store and LVF) when any discrepancy in a database is found. The discrepancy reporting audience is anyone who is using the data and finds a problem.

Term or Abbreviation (Expansion)	Definition / Description
DSP (Digital Signal Processing)	Digital Signal Processing is the use of computers, or more specialized digital signal processors, to analyze a digital stream of information to perform error detection, data compression, or other application specific manipulations.
DSCP (Differentiated Services Code Point)	A DSCP is a packet header value that can be used to request high priority or best effort delivery for traffic on an IP network.
DTMF (Dual Tone Multi-Frequency) also known as Touch-Tone™	The transmission of a selected number or symbol (*, #) via the generation of a specific pair of tones when that number's or symbol's button on a push button telephone is pressed. The tones are audible and transmitted within the voice band.
ECRF (Emergency Call Routing Function)	A functional element in an ESInet which is a LoST protocol server where location information (either civic address or geo-coordinates) and a Service URN serve as input to a mapping function that returns a URI used to route an emergency call toward the appropriate PSAP for the caller's location or towards a responder agency. • External ECRF: An ECRF instance that resides outside of an ESInet instance. • Internal ECRF: An ECRF instance that resides within and is only accessible from an ESInet instance.
EIDO (Emergency Incident Data Object)	A standardized JSON object used by NG9-1-1 Functional Elements and Services for exchanging Incident-related data.
EMS (Emergency Medical Service)	A service providing out-of-hospital acute care and transport to definitive care, to patients with illnesses and injuries which the patient believes constitute a medical emergency.
EO (End Office)	The Local Exchange Carrier facility where access lines are connected to switching equipment for connection to the Public Switched Telephone Network.

Term or Abbreviation (Expansion)	Definition / Description
ESInet (Emergency Services IP Network)	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 services can be deployed, including, but not restricted to, those necessary for providing NG9-1-1 services. ESInets may be constructed from a mix of dedicated and shared facilities. ESInets may be interconnected at local, regional, state, federal, national and international levels to form an IP-based inter-network (network of networks). The term ESInet designates the network, not the services that ride on the network. See NG9-1-1 Core Services.
ESRP (Emergency Services Routing Proxy)	An i3 functional element which is a SIP proxy server that selects the next hop routing within the ESInet based on location and policy. There is an ESRP on the edge of the ESInet. There is usually an ESRP at the entrance to an NG9-1-1 PSAP. There may be one or more intermediate ESRPs between them. • Originating ESRP: The first routing element within the Next Generation Core Services (NGCS). It receives calls from the BCF at the edge of the ESInet. Terminating ESRP: The last ESRP for a call in NGCS.
ESS (External Switching Systems)	The administrative, non-emergency communications systems within the PSAP serve as external switching systems for telephony and other administrative communications (voice mail, email, instant messaging, etc.). The ESS equipment might be represented by a traditional PBX or other communications gateway.

Term or Abbreviation (Expansion)	Definition / Description
FCC	The FCC is an independent agency of the United States government, created and overseen by Congress to regulate interstate communications by radio, television, wire, satellite, and cable in all 50 states, the District of Columbia and U.S. territories. For details see: https://www.fcc.gov/
FE (Functional Element) ***AKA: Functional Entity***	A set of software features that may be combined with hardware interfaces and operations on those interfaces to accomplish a defined task.
FIPS (Federal Information Processing Standards)	Federal Information Processing Standards (FIPS) are publicly announced standards developed by the United States federal government for use in computer systems by non-military government agencies and government contractors. Refer to FIPS in Wikipedia for overall information County & County Equivalent Codes: https://www.census.gov/library/reference/code-lists/ansi.html#par_statelist describes the names and codes that represent the counties and equivalent legal and/or statistical subdivisions (i.e., counties) of the 50 states, the District of Columbia, and the possessions. Security Requirements for Cryptographic Modules https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf describes document processing, encryption algorithms and other information technology standards for use within non-military government agencies and by government contractors and vendors who work with the agencies. The standards cover a specific topic in information technology (IT) and strive to achieve a common level of quality or interoperability.

Term or Abbreviation (Expansion)	Definition / Description
Fusion Center	A state or major urban area focal point established for the receipt, analysis, gathering, and sharing of threat-related information between federal; state, local, tribal, territorial (SLTT); and private sector partners. https://www.dhs.gov/state-and-major-urban-area-fusion-centers
GIS (Geographic Information System)	A system for capturing, storing, displaying, analyzing and managing data and associated attributes which are spatially referenced.
HELD (HTTP Enabled Location Delivery)	A protocol that can be used to acquire Location Information (LI) from a LIS within an access network as defined in IETF RFC 5985.
HIPAA (Health Insurance Portability and Accountability Act)	A federal law that amended the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.
ICMP (Internet Control Message Protocol)	ICMP is a supporting protocol in the Internet protocol suite and is used by network devices, including routers, to send error messages and operational information indicating, for example, that a requested service is not available or that a host or router could not be reached.
IDPS (Intrusion Detection and Prevention Systems) or IDS (Intrusion Detection System)	An IDPS or IDS is a device or software application that monitors a network or systems for malicious activity or policy violations. Any malicious activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system.
IDX (Incident Data Exchange)	An Incident Data Exchange (IDX) is a functional element that aggregates EIDO information from multiple FEs within an agency and creates a composite EIDO that represents the entire state of an incident as known by the agency at the time the aggregated EIDO was sent by the IDX.

Term or Abbreviation (Expansion)	Definition / Description
IMR (Interactive Media Response)	An automated service used to play announcements, record responses and interact with callers using any or all of audio, video and text.
IoT (Internet of Things)	IoT is the network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and connectivity which enables these things to connect and exchange data, creating opportunities for more direct integration of the physical world into computer-based systems.
IP (Internet Protocol) ***AKA: TCP/IP***	A communications protocol linking different computer platforms across networks. TCP/IP functions at the 3rd and 4th levels of the Open Systems Interconnection model.
IPS (Intrusion Prevention System)	IPS is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits.
ISCM (Information Security Continuous Monitoring)	ISCM, developed by the US National Institute of Standards and Technology (NIST), provides detailed guidance on implementing a risk management framework and a detailed control set for federal agencies to adopt to establish a continuous monitoring plan.
ISDN (Integrated Services Digital Network)	International standard for a public communication network to handle circuit-switched digital voice, circuit-switched data, and packet-switched data.
JMX (Java Management Extensions)	Java Management Extensions (JMX) is a Java technology that supplies tools for managing and monitoring applications, system objects, devices (such as printers) and service-oriented networks.
KRACK (Key Reinstallation Attack)	KRACK ("Key Reinstallation Attack") is a severe replay attack (a type of exploitable flaw) on the Wi-Fi Protected Access protocol that secures Wi-Fi connections.
LNG (Legacy Network Gateway)	An NG9-1-1 Functional Element that provides an interface between a non-IP originating network and a Next Generation Core Services (NGCS) enabled network.

Term or Abbreviation (Expansion)	Definition / Description
LoST	A protocol that takes location information and a Service URN and returns a URI. Used generally for location-based call routing. In NG9-1-1, used as the protocol for the ECRF and LVF.
LPG (Legacy PSAP Gateway)	The Legacy PSAP Gateway is a signaling and media interconnection point between an ESInet and a legacy PSAP. It plays a role in the delivery of emergency calls that traverse an i3 ESInet to get to a legacy PSAP, as well as in the transfer and alternate routing of emergency calls between legacy PSAPs and NG9-1-1 PSAPs. The Legacy PSAP Gateway supports an IP (i.e., SIP) interface towards the ESInet on one side, and a traditional MF or Enhanced MF interface (comparable to the interface between a traditional Selective Router and a legacy PSAP) on the other.
LSRG (Legacy Selective Router Gateway)	The LSRG provides an interface between a 9-1-1 Selective Router and an ESInet, enabling calls to be routed and/or transferred between Legacy and NG networks. A tool for the transition process from Legacy 9-1-1 to NG9-1-1.
LVF (Location Validation Function)	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.
MDS (Mapping Data Service)	Provides a PSAP call taker with information showing the location of an out-of-area caller
MF (Multi-Frequency)	A type of in-band signaling used on analog interoffice and 9-1-1 trunks.
MIS (Management Information System)	A program that collects, stores and collates data into reports enabling interpretation and evaluation of performance, trends, traffic capacities, etc.

Term or Abbreviation (Expansion)	Definition / Description
MSAG (Master Street Address Guide)	A database of street names and house number ranges within their associated communities defining Emergency Service Zones (ESZs) and their associated Emergency Service Numbers (ESNs) to enable proper routing of 9-1-1 calls.
NASNA (National Association of State 9-1-1 Administrators)	An association that represents state 9-1-1 programs in the field of emergency communications. http://www.nasna911.org/.
NCIC (National Crime Information Center)	An FBI (Federal Bureau of Investigation) computerized index of criminal justice information (i.e. - criminal record history information, fugitives, stolen properties, missing persons). It is available to Federal, state, and local law enforcement and other criminal justice agencies and is operational 24 hours a day, 365 days a year. https://www.fbi.gov/services/cjis/ncic.
NENA (National Emergency Number Association)	The National Emergency Number Association is a not-for-profit corporation established in 1982 to further the goal of "One Nation-One Number." NENA is a networking source and promotes research, planning and training. NENA strives to educate, set standards and provide certification programs, legislative representation and technical assistance for implementing and managing 9-1-1 systems. https://www.nena.org/

Term or Abbreviation (Expansion)	Definition / Description
NG9-1-1	"Next Generation 9-1-1 services" means a secure, IP-based, open-standards system comprised of hardware, software, data, and operational policies and procedures that: (A) provides standardized interfaces from emergency call and message services to support emergency communications; (B) processes all types of emergency calls, including voice, text, data, and multimedia information; (C) acquires and integrates additional emergency call data useful to call routing and handling; (D) delivers the emergency calls, messages, and data to the appropriate public safety answering point and other appropriate emergency entities based on the location of the caller; (E) supports data, video, and other communications needs for coordinated incident response and management; and (F) interoperates with services and networks used by first responders to facilitate emergency response. REF: Agreed to by NENA, NASNA, iCERT, and the National 9-1-1 Office representatives on 01/12/2018.
NGCS (Next Generation 9-1-1 (NG9-1-1) Core Services)	The base set of services needed to process a 9-1-1 call on an ESInet. Includes the ESRP, ECRF, LVF, BCF, Bridge, Policy Store, Logging Services and typical IP services such as DNS and DHCP. The term NG9-1-1 Core Services includes the services and not the network on which they operate. See Emergency Services IP Network.
NHTSA (National Highway Traffic Safety Administration)	The National Highway Traffic Safety Administration is an agency of the Executive Branch of the U.S. government, part of the Department of Transportation. It describes its mission as "Save lives, prevent injuries, reduce vehicle-related crashes." The National 9-1-1 Program is housed under NHTSA. https://www.nhtsa.gov/

Term or Abbreviation (Expansion)	Definition / Description
NIST (National Institute of Standards and Technology)	A part of the United States Department of Commerce that oversees the operation of the U.S. National Bureau of Standards. NIST works with industry and government to advance measurement science and to develop standards in support of industry, commerce, scientific institutions, and all branches of government. Their mission is to promote innovation and industrial competitiveness. https://www.nist.gov
NMS (Network Management System)	A class of software that used to monitor and manage network infrastructure and attached devices using standard and non-standard protocols.
NOC (Network Operations Center)	A network operations center (NOC, pronounced like the word knock), also known as a "network management center", is one or more locations from which network monitoring and control, or network management, is exercised over a computer, telecommunication or satellite network.
NTP (Network Time Protocol)	A networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.
OSP (Originating Service Provider)	A communications entity providing a network that allows users or subscribers to originate 9-1-1 voice or non-voice messages from the public to a 9-1-1 Authority. The network includes the access network and the calling network.
OTT (Over-The-Top)	Communications between applications or devices over a network service where the network service only provides the transmission facilities and is not actively involved in the application-level messaging.
PBX (Private Branch Exchange)	A private telephone switch that is connected to the Public Switched Telephone Network.
PIO (Public Information Office)	The person(s) responsible for communications or spokespersons of organizations.

Term or Abbreviation (Expansion)	Definition / Description
PKI (Public Key Infrastructure)	A set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.
PRF (Policy Routing Function)	That functional component of an Emergency Services Routing Proxy that determines the next hop in the SIP signaling path using a policy.
PSAP (Public Safety Answering Point)	An entity responsible for receiving 9-1-1 calls and processing those calls according to a specific operational policy. • Primary PSAP: A PSAP to which 9-1-1 calls are routed directly from the 9-1-1 Control Office. • Secondary PSAP: A PSAP to which 9-1-1 calls are transferred from a Primary PSAP. • Alternate PSAP: A PSAP designated to receive calls when the primary PSAP is unable to do so. • Consolidated PSAP: A facility where multiple Public Safety Agencies choose to operate as a single 9-1-1 entity. • Legacy PSAP: A PSAP that cannot process calls received via i3-defined call interfaces (IP-based calls) and still requires the use of CAMA or ISDN trunk technology for delivery of 9-1-1 emergency calls. • Serving PSAP: The PSAP to which a call would normally be routed. NG9-1-1 PSAP: A PSAP capable of processing calls and accessing data services as defined in NENA's i3 specification, NENA-STA-010, and referred to therein as an "i3 PSAP".
PSTN (Public Switched Telephone Network)	The network of equipment, lines, and controls assembled to establish communication paths between calling and called parties in North America.
PTT (Push-to-Talk)	Push-to-Talk (PTT) is a method of communication by which a user initiates a request to talk to another user or group of users in real-time, on demand by activating a function on their subscriber device.

Term or Abbreviation (Expansion)	Definition / Description
PTToC	A service that operates over a cellular network where the user pushes a button on the device to transmit, often used to replace or extend traditional two-way radio service.
RFC (Request for Comment)	A method by which standard setting bodies receive input from interested parties outside of the working group.
SAR (Suspicious Activity Report)	A SAR is official documentation of observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity.
SBC (Session Border Controller)	A commonly available functional element that provides security, NAT traversal, protocol repair and other functions to VoIP signaling such as SIP. A component of a Border Control Function.
SIP (Session Initiation Protocol)	A protocol specified by the IETF (RFC 3261) that defines a method for establishing multimedia sessions over the Internet. Used as the call signaling protocol in VoIP, NENA i2 and NENA i3.
SLA (Service Level Agreement)	A service level agreement (SLA) is a contract between a service provider (either internal or external) and the end user that defines the level of service expected from the service provider. SLAs are output-based in that their purpose is specifically to define what the customer will receive.
SNMP (Simple Network Management Protocol)	A protocol defined by the IETF used for managing devices on an IP network.
SOC (Security Operations Center)	A centralized operating unit that deals with security issues on an organizational and technical level.
SR (Selective Router) AKA: Enhanced 9-1-1 Control Office	The Central Office that provides the tandem switching of 9-1-1 calls. It controls delivery of the voice call with ANI to the PSAP and provides Selective Routing, Speed Calling, Selective Transfer, Fixed Transfer, and certain maintenance functions for each PSAP.

Term or Abbreviation (Expansion)	Definition / Description
SRC (Session Recording Client)	The Logging Service acts as a Session Recording Server (SRS), and accepts media and metadata from a Session Recording Client (SRC).
SRTP (Secure Real Time Protocol)	An IP protocol used to securely transport media (voice, video, text) which have a real-time constraint.
TDM (Time Division Multiplexing)	A digital multiplexing technique for combining a number of signals into a single transmission facility by interweaving pieces from each source into separate time slots.
TDoS (Telephone Denial of Service)	Illegal attacks targeting the telephone network by generating numerous phone calls, tying up the network and preventing an agency from receiving legitimate calls.
TFOPA (Task Force on Optimal PSAP Architecture)	The FCC organized a group of industry professionals into a Task Force on Optimal Public Safety Answering Point (PSAP) Architecture. TFOPA was directed to study and report findings and recommendations on 9-1-1 structure and architecture in order to determine whether additional consolidation of PSAP infrastructure and architecture improvements would promote greater efficiency of operations, safety of life, and cost containment, while retaining needed integration with local first responder dispatch and support.
TIA (Telecommunications Industry Association)	A lobbying and trade association, the result of the merger of the USTA (United States Telephone Association) and the EIA (Electronic Industries Association).
URL (Uniform Resource Locator)	A URL is a type of URI, specifically used for describing and navigating to a resource (e.g., https://www.nena.org/)
USB (Universal Serial Bus)	USB is an industry standard that establishes specifications for cables, connectors and protocols for connection, communication and power supply between personal computers and their peripheral devices.

Term or Abbreviation (Expansion)	Definition / Description
US-CERT (United States Computer Emergency Readiness Team)	An organization within the Department of Homeland Security whose mission is to support and monitor information that assists agencies to reduce the risk of systemic cybersecurity and communications challenges.
VOIP (Voice over Internet Protocol)	Technology that permits delivery of voice calls and other real-time multimedia sessions over IP networks.
VPN (Virtual Private Network)	A network implemented on top of another network, and private from it, providing transparent services between networks or devices and networks. VPNs often use some form of cryptographic security to provide this separation.
WAN (Wide Area Network)	A wide area network (WAN) is a computer network that spans a relatively large geographical area and consists of two or more interconnected local area networks (LANs).
WiFi ®	A wireless networking technology that uses radio waves to provide wireless high-speed internet and network connections. Wi-Fi is a registered trademark phrase that means IEEE 802.11x.
WIPS (Wireless Intrusion Protection System)	WIPS is a network device that monitors the radio spectrum for the presence of unauthorized access points and can automatically take countermeasures.
WLAN (Wireless Local Area Network)	A wireless LAN is a wireless computer network that links two or more devices using wireless communication to form a local area network (LAN) within a limited area such as a home, school, computer laboratory, campus, office building etc.
WMI (Windows Management Instrumentation)	Windows Management Instrumentation is a set of specifications from Microsoft for consolidating the management of devices and applications in a network from Windows computing systems.
WPA (Wi-Fi Protected Access)	Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. WPA (sometimes referred to as the draft IEEE 802.11i standard) became available in 2003.

4 Recommended Reading and References

[1] National Emergency Number Association. *Master Glossary of 9-1-1 Terminology.* NENA-ADM-000.22-2018. Arlington, VA: NENA, approved April 13, 2018,

[2] National Emergency Number Association. *i3 Standard for Next Generation 9-1-1*. NENA-STA-010.3-20xx. Arlington, VA: NENA, (forthcoming).

[3] National Emergency Number Association. *Emergency Services IP Network Design (ESIND)*. NENA-INF-016.2-2018. Arlington, VA: NENA, approved April 5, 2018.

[4] Internet Engineering Task Force. *Network Configuration Protocol (NETCONF)*. RFC 6241, June 2011.

[5] Association of Public Safety Communications Officials and National Emergency Number Association. Service Capability Criteria Rating Scale, APCO/NENA ANS 1.102.2-2010. Arlington, VA: NENA, approved July 28, 2010.

[6] Department of Homeland Security, Federal Emergency Management Agency. *Continuity of Operations Plan Template for Federal Departments and Agencies.* Washington DC: FEMA, April 2013.

[7] Department of Homeland Security. "Continuous Diagnostics and Mitigation" (website). https://www.us-cert.gov/cdm/home.

[8] National Emergency Number Association. *Technical Information Document Network/System Access Security.* NENA 04-503. Arlington, VA: NENA, approved December 1, 2005.

[9] National Emergency Number Association. *Security for Next-Generation 9-1-1 Standard (NG-SEC).* NENA 75-001. Arlington, VA: NENA, approved February 6, 2010.

[10] National Emergency Number Association. *NG9-1-1 Security Information Document*, NENA-INF-015.1-2016. Arlington, VA: NENA, approved December 8, 2017.

[11] National Emergency Number Association. *Next Generation 9-1-1 Security (NG-SEC) Audit Checklist*. NENA 75-502. Arlington, VA: NENA, approved December 14, 2011.

[12] Association of Public Safety Communications Officials. *An Introduction to Cybersecurity – A Guide for PSAPs*. An Introduction to Cybersecurity. Daytona Beach, FL: APCO, July 2016.

[13] National Institute of Standards and Technology. *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems.* NIST Special Publication 800-160, Systems Security Engineering.

[14] U.S. Department of Justice, Federal Bureau of Investigation. *Criminal Justice Information Services (CJIS) Security Policy.* CJISD-ITS-DOC-08140-5.8. Washington, DC: USDOJ, June 1, 2019.

[15] Department of Homeland Security. "Sharing Critical Information to Protect the Networks and Systems We All Rely Upon." Cybersecurity & Infrastructure Security Agency (CISA). October 31, 2017.

https://www.dhs.gov/cisa/blog/2017/10/31/sharing-critical-information-protect-networks-and-systems-we-all-rely-upon.

[16] Department of Homeland Security. "The Continuing Denial of Service Threat Posed by DNS Recursion (v2.0)". U.S. Computer Emergency Readiness Team (US-CERT). Revised February 6, 2013. https://www.us-cert.gov/security-publications/continuing-denial-service-threat-posed-dns-recursion-v20.

[17] Telecommunications Industry Association (TIA). *A Telecommunications Infrastructure Standard for Data Centers*. ANSI/TIA-942-A. Arlington, VA: TIA, approved August 2, 2012.

[18] National Emergency Number Association. *PSAP Site Characteristics Information Document*. NENA-INF-024.2-2018 (originally 04-502). Arlington, VA: NENA, approved February 14, 2018.

[19] National Highway Traffic Safety Administration (NHTSA). "Revision of Model State 911 Plan and Guidelines for State NG911 Legislative Language". National 911 Office. Washington, DC: NHTSA. Version 2.0, 2018. https://www.911.gov/project_911modellegislativeguidelines.html.

[20] Department of Homeland Security. "Governance Resources". SAFECOM. Washington, DC: SAFECOM. https://www.dhs.gov/safecom/governance.

[21] National Emergency Number Association. *GIS Data Stewardship for Next Generation 9-1-1.* NENA-INF-028-2020.

[22] National Emergency Number Association. *NENA Standard for NG9-1-1 GIS Data Model*. NENA-STA-006.1-2018. Arlington, VA: NENA, approved June 6, 2018.

[23] National Emergency Number Association. *NENA Standards for the Provisioning and Maintenance of GIS data to ECRF and LVFs.* NENA-STA-005.1.1-2017. Arlington, VA: NENA, approved August 10, 2017.

[24] National Emergency Number Association. *NG9-1-1 Call Processing Metrics Standard*. NENA-STA-019.1-2018. Arlington, VA: NENA, approved July 2, 2018.

[25] Department of Homeland Security. "Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Version 1.5.5". National Criminal Intelligence Resource Center (U.S.). ISE-FS-200. Washington, DC: DHS, February 23, 2015.

[26] National Emergency Number Association. *NG9-1-1 PSAP Standard.* NENA-STA-023.1-20xx. Arlington, VA: NENA, (forthcoming).

[27] Disruptions to Communications. 47 C.F.R. § 4.

[28] Resiliency, Redundancy and Reliability of Communications. 47 C.F.R. § 12.

[29] Federal Communications Commission. "Task Force on Optimal Public Safety Answering Point Architecture." Public Safety and Homeland Security Bureau. Updated December 7, 2016. https://www.fcc.gov/about-fcc/advisory-committees/general/task-force-optimal-public-safety-answering-point.

[30] National Emergency Number Association, National Association of State 911 Administrators, and Industry Council for Emergency Response Technologies. *Recommended Best Practices for Supplemental 9-1-1 Location Data.* Arlington, VA: NENA, February 2019.
[31] Department of Homeland Security. *Improving the Cybersecurity Posture of NG911 Systems*. SAFECOM. Washington, DC: SAFECOM. https://www.dhs.gov/safecom/blog/2016/04/01/improving-cybersecurity-posture-ng911-systems
[32] National Institute of Standards and Technology. *Guide for Conducting Risk Assessments.* NIST Special Publication 800-30, Revision 1. , Guide for Conducting Risk Assessments. September 2012.
[33] Department of Homeland Security. "Cybersecurity Assessments". Cybersecurity and Infrastructure Security Agency. https://www.us-cert.gov/resources.
[34] Association of Public Safety Communications Officials. *Telephony Denial of Services (TDOS) to Public Safety Communications Phone Service*. Daytona Beach, FL: APCO, March 28, 2013.
[35] General Accountability Office. "Critical Infrastructure Protection: More Comprehensive Planning Would Enhance the Cybersecurity of Public Safety Entities' Emerging Technology". GAO-14-125. Washington, DC: GAO, January 28, 2014.
[36] National Institute of Standards and Technology. *Glossary of Key Information Security Terms.* NISTIR 7298, Rev. 3. Washington, DC: NIST, April 16, 2018.
[37] National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*. Washington, DC: NIST, July 2019.
[38] Exec. Order No. 13,636, 78 Fed. Reg. 11737 (February 12, 2013).
[39] National Institute of Standards and Technology. *Guide for Mapping Types of Information and Information Systems to Security Categories (2 vols.).* Special Publication (NIST SP) - 800-60 Rev 1. Kevin M. Stine, Richard L. Kissel, William C. Barker, Annabelle Lee, J Fahlsing, Jessica Gulick, August 1, 2008.
[40] National Institute of Standards and Technology. *Standards for Security Categorization of Federal Information and Information Systems*. FIPS 199. February 2004.
[41] Department of Homeland Security. "Critical Infrastructure Cyber Community (C³) Voluntary Program". August 22, 2018. https://www.dhs.gov/ccubedvp.
[42] Department of Homeland Security. "Events and Media". https://www.us-cert.gov/resources/events.
[43] National Institute of Standards and Technology. *An Introduction to Information Security*. SP 800-12, Revision 1. Michael Nieles (NIST), Kelley Dempsey (NIST), Victoria Pillitteri (NIST), June 2017.
[44] National Institute of Standards and Technology. *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*. SP 800-137.

Kelley Dempsey (NIST), Nirali Chawla (PwC), L. Johnson (NIST), Ronald Johnston (DoD), Alicia Jones (BAH), Angela Orebaugh (BAH), Matthew Scholl (NIST), Kevin Stine (NIST), September 2011.

[45] National Institute of Standards and Technology. *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*. Special Publication (NIST SP) - 800-53A Rev 4. Ronald S. Ross, December 11, 2014.

[46] National Emergency Number Association. *Emergency Incident Data Object (EIDO).* NENA-STA-021.1-201X. Arlington, VA: NENA, forthcoming).

[47] Association of Public-Safety Communications Officials and Central Station Alarm. Association. *Automated Secure Alarm Protocol.* APCO/CSAA ANS 2.101.2 2014. Daytona Beach, FL: APCO, approved August 5, 2014.

[48] Internet Engineering Task Force. *Session Initiation Protocol Event Package for Voice Quality Reporting.* A. Pendleton, A. Clark, A. Johnston, H. Sinnreich. RFC 6035, November 2010.

5 Exhibit

None.

6 Appendix

None.

7 ACKNOWLEDGEMENTS

The National Emergency Number Association (NENA) Agency Systems Committee, Monitoring and Managing NG9-1-1 Working Group developed this document.

NENA Board of Directors Approval Date: 08/19/2020

NENA recognizes the following industry experts and their employers for their contributions to the development of this document.

Members	Employer
Michael Smith, Agency Systems Co-Chair and Working Group Co-Chair	Equature/DSS, Corp.
Rick Blackwell, ENP, Agency Systems Co-Chair and Working Group Co-Chair	Greenville County, SC
Steve McMurrer, ENP, Technical Editor	Fairfax County, VA
Bernard Brabant	Consultant
Maria Jacques, ENP	State of Maine
Christian Militeau, ENP	Intrado
Beverly Wolfe Davis	City of Memphis, TN
Tommy Tran	North Central Texas 9-1-1
Michael Vislocky	Network Orange, Inc.
Lisa Wirtanen	AT&T
Chuck Townsend, ENP	Consultant
David Hopkins	Steuben County, NY
Roger Hixson, ENP	NENA
Shelly Guenther	NGA 911 LLC
Robert Kujawa	Northbrook IL Police Department
Roger Marshall	Comtech Telecommunications Corporation
Robert Woodhull	Pinal County, AZ
Justin Prahar	ECaTS
Audrey Kenny	Bucks County, PA
Guy Caron	Bell Canada
Deirdre Garrett-Harris	City of Dallas, TX
Linda Ogilvie	Consultant, Linda Ogilvie
Alice Johnson	Zetron, Inc.
Chris Robinson, GISP	Michael Baker International
Jeff Wheeler	Data Technical Services
Travis LePage	Federal Engineering, Inc.

Special Acknowledgements:

Delaine Arnold, ENP, Committee Resource Manager, has facilitated the production of this document through the prescribed approval process.

The Monitoring and Managing NG9-1-1 Working Group is part of the NENA Development Group that is led by:

- Jim Shepard, ENP, and Wendi Rooney, ENP, Development Steering Council Co-Chairs
- Brandon Abley, ENP, Technical Issues Director
- April Heinze, PSAP Operations Director