A Forward-Looking Approach to
EMERGENCY COMMUNICATIONS

APCO International

APCO International's Definitive Guide to NEXT GENERATION 9·1·1

APCO International's Definitive Guide to

NEXT GENERATION 9·1·1

A Forward-Looking Approach to Emergency Communications

Contents

Introduction

While the nation's 9-1-1 systems have accommodated several changes in technology and the way the public communicates, systems largely use more than 50-year-old technology. What does "Next Generation 9-1-1" mean for ECCs? Major changes are coming. Understanding important concepts associated with NG9-1-1 is essential.

What Is NG9-1-1?

NG9-1-1 has been discussed for more than a decade, but it's only in recent years that the nation's largest public safety organizations have reached consensus on how to define NG9-1-1 in a way that aligns with core public safety principles like interoperability, security, and innovation. In contrast to how NG9-1-1 was first conceptualized, NG9-1-1 should not be narrowly defined as a digital, IP network that connects 9-1-1 callers and ECCs. (In other words, NG9-1-1 is more than a collection of emergency services IP networks, or ESInets.)

NG9-1-1 needs to mean the ability of ECCs to receive new forms of data from the public; process, triage, and analyze this information; and share incident data in a fully interoperable manner with other ECCs and responders in the field. ECCs should have whatever technologies and capabilities are required to interact with the public and responders in the field.

Progress toward NG9-1-1, even by just establishing digital connections between callers and ECCs, has unfortunately been hindered by many of the same challenges public safety agencies have historically faced with technology deployments. ECCs are dealing with customized, proprietary solutions that in many cases fail to provide the operational capabilities promised, inflate costs, and lock agencies into non-interoperable solutions. This is unacceptable. Acting individually, even at the state level, the 9-1-1 community faces significant obstacles to overcoming the status quo, but collectively, ECCs working toward a common vision of NG9-1-1, can break the cycle.

What Is in This Guide?

This guide is intended to fill a gap in resources available to ECCs by providing explanations and recommendations based on a comprehensive understanding of what NG9-1-1 means and ECCs' experiences with efforts to deploy precursors to NG9-1-1. Other resources focus on technical aspects of NG9-1-1 call flow or take a broader perspective of broadband implications for ECCs. This guide builds upon those resources to help ECCs make decisions *today* on a variety of issues – procurement, budgeting, hiring, training, etc. – and brings a common understanding of how to move forward.

APCO offers this guide to support our members and the broader public safety community. In some respects, this guide will require readers to set aside current assumptions about the way things are being done today. Most fundamentally this guide is written from the perspective of what ECCs and public safety telecommunicators (PSTs) need. ■


to the future

Chapter 1
The Coming Transformation

The purpose of this guide is to establish a foundation for understanding all facets of NG9-1-1, from basics such as key definitions to comparisons with efforts underway to implement precursor technologies and capabilities. To set the stage, a very abbreviated history of 9-1-1 in the United States is prudent. It is important to understand how things stand today and highlight the contrasts with NG9-1-1 and the challenges to overcome.

9-1-1 History in Context

PSTs have been providing highly skilled and professional services to 9-1-1 callers for more than 50 years. The first 9-1-1 call was made in 1968, creating the opportunity to leverage the technology of that era to provide the public with a streamlined way to call for help.

The advent of cellular telephones presented new challenges to emergency communications centers (ECCs). The caller was no longer tethered to a known and fixed location, as was initially the case for landline telephones. Wireless service providers essentially piggybacked on the existing NG9-1-1 network but had to develop additional capabilities to route the call based on the cell tower handling the call and provide rudimentary location information. ECCs began receiving Wireless Phase 1 location information, which indicated the location of the cell tower or cell sector a caller was connected to. As network and cellular device technology evolved, Wireless Phase 2 gave the ECC a more granular estimated location of the caller.

Eventually, cellular carriers enabled short message service (SMS) text capabilities and extended this to 9-1-1. Initial implementations were not interoperable among text-to-911 service providers, meaning ECCs had difficulty transferring text-based requests for emergency assistance, and little to no location information was available. Additionally, texts were often converted to TTY or processed using a web interface, which presented challenges. As should be expected, some of these limitations have been overcome, and more ECCs have integrated text-to-911 into their Customer Premises Equipment (CPE).

It is important to understand how things stand today and highlight the contrasts with NG9-1-1 and the challenges to overcome.

ECCs have also been able to receive supplemental information related to emergency incidents from automotive telematics (example – crash notifications), alarm monitoring services via the Automated Secure Alarm Protocol (ASAP),[1] and other emergency alerting systems, often directly into their CPE and computer aided dispatch (CAD) equipment.

More Recent Developments

Wireless caller location accuracy has improved, particularly in the horizontal plane for calls made outdoors. Wireless carriers, however, have yet to uniformly provide PSTs with actionable location information (dispatchable location) for 9-1-1 calls made inside buildings. Wireless call routing is increasingly becoming more precise, with routing decisions being based on the location of the device versus the location of the cell tower antenna sector, which helps reduce the need for call transfers that were particularly common near jurisdictional boundaries. Some wireless carriers are implementing location-based routing without imposing costs on 9-1-1 authorities and regardless of any precursor NG9-1-1 deployments (such as ESInets).

Another development of note is how new technology companies serving ECCs are offering over-the-top (OTT) applications that bypass the limitations of today's legacy, analog 9-1-1 network. PSTs access these capabilities via onsite and cloud-based, hosted solutions. Sometimes these applications require a new dedicated screen, but increasingly they can be integrated into existing call-handling solutions and CAD interfaces. Features include enhanced caller location, the ability to enable the caller to share photos and live video, and access to other data sources such as weather information, traffic, social media, etc. While these offerings do help to increase situational awareness and improve response capabilities, they generally face limitations from operating outside of the 9-1-1 network, and, in many cases, they are not interoperable with other providers, CPE and CAD systems.

There is a lot of confusion about what "NG9-1-1" means, and much progress to date amounts to piecemeal solutions that are either tied down by old technology or bypass the 9-1-1 network altogether.

One constant has been the perseverance of our PSTs. Despite a 9-1-1 infrastructure that has essentially remained unchanged from its 1960s-era roots, ECCs have experienced the development of new communications technologies made available to the public. PSTs' roles have evolved with these technologies. In many ways, these types of changes make an already difficult job even harder.

Several 9-1-1 authorities at the state and local levels have been hard at work modernizing the 9-1-1 network to NG9-1-1. There is a lot of confusion about what "NG9-1-1" means, and much progress to date amounts to piecemeal solutions that are either tied down by old technology or bypass the 9-1-1 network altogether. Unfortunately, 9-1-1 authorities and ECCs are facing problems all too familiar to the public safety community, most notably a lack of interoperability due to proprietary implementations. ECCs deserve better. Solutions need to be reliable, intuitive, integrated, and interoperable.

Chapter 1

KEY TAKEAWAYS

- 9-1-1 has evolved but in many ways is **still using 1960s technology**.
- ECCs' communications capabilities **do not match those of the public**.
- Over-the-top (OTT) applications are providing **"Next Gen" data to some ECCs**.
- There are **significant benefits when solutions are interoperable and fully integrated** with the 9-1-1 system.

[1] ASAP to PSAP - APCO International (apcointl.org)

Chapter 2
Key Technology Concepts

A shared understanding of what NG9-1-1 means is essential to making real progress throughout the country. It is generally understood that NG9-1-1 will enable ECCs to receive more than just "calls," with new requests for emergency services, including IP-based voice and messaging, pictures, videos, and many other types of multimedia and data. There will be "non-human initiated" inputs such as information from automated devices, sensors, telematics, and the Internet of Things (IoT).

A shared understanding of what NG9-1-1 needs to mean is essential to making real progress throughout the country.

But NG9-1-1 is not just about enabling new inputs into ECCs. Thinking of NG9-1-1 must be in a comprehensive, end-to-end fashion. NG9-1-1 needs to mean: the ability of ECCs to receive new forms of data from the public; process, triage, and analyze this information; and share incident data in a fully interoperable manner with other ECCs and responders in the field. Described this way, NG9-1-1 does not yet exist anywhere in the country.

The Role of Interoperability

Interoperability is the key to the success of NG9-1-1 and must be properly defined. National public safety associations[2] have devised the most complete definition of "interoperability" as applicable to NG9-1-1: the capability of ECCs to receive 9-1-1 requests for emergency assistance, then process and share this information with other ECCs and emergency response providers without the need for proprietary interfaces and regardless of jurisdiction, equipment, device, software, service provider, or other relevant factors. Unfortunately, ESInet deployments lack interoperability, and we must change course to truly achieve NG9-1-1.

The public relies on PSTs to take information about an emergency, determine what resources are required, and share any necessary data and information with responder agencies throughout the incident.

ECCs' capabilities should align with the experience and expectations of the public. Consumers today use more connected devices (including smartphones, tablets, gaming devices, etc.) and are sharing all types of data with each other. Regardless of the service provider, device, and manufacturer, the public can for the most part communicate and exchange information directly and without delay through various applications and services. The public should rightly expect ECCs to do the same. The public relies on PSTs to take information about an emergency, determine what resources are required, and share any necessary data and information with responder agencies throughout the incident. Thus, interoperability must be a fundamental aspect of NG9-1-1. The ability to seamlessly access and share all available data will allow the PST to readily analyze the information, gain situational awareness, and determine the priority of resources necessary for the reported incident.

Interoperability also enables other key NG9-1-1 capabilities. When implemented in an interoperable manner, NG9-1-1 provides new opportunities for ECC backup, remote call handling and dispatch, and tactical deployments. Having an alternate ECC capable of receiving emergency calls for service with the same capabilities as the primary ECC during a

planned or unplanned event is essential. IP-based systems through mobile broadband providers such as FirstNet have extended networks beyond the traditional ECC structure for new remote call handling and dispatch capabilities. ECCs can establish field-based operations during natural or man-made disasters.

Accelerating Innovation

The benefits of NG9-1-1 will extend well beyond the delivery of new forms of information to ECCs. The increased amount of data, when managed with recent innovations such as data and video analytics products and social media mining and aggregation tools, will provide new opportunities for real-time analysis of active incidents, leading to enhanced situational awareness for 9-1-1 professionals and emergency responders.

The burgeoning IoT will present new opportunities for ECCs. An increasing number of low-cost and low-power internet-connected devices are becoming embedded in everyday objects, public safety vehicles, devices carried by field-based first responders, transportation infrastructure, utility grids, water and sewer services. These IoT devices have the potential to send and receive data important to emergency response and safety of life and property to NG9-1-1 ECCs and other public safety systems.

To deal with the increased amounts of information, new tools can prevent PST overload and assist with processing. For example, IoT devices can include access to cloud-based analytics and machine learning to improve the information provided to the PST. Artificial intelligence (AI) solutions can offer predictive analysis and improve the quality of data and ECC operations. AI can assist in prioritizing calls and triaging non-emergency calls to manage the dispatch of field-based responders more effectively. AI can also play a role in quality assurance/improvement and customer service.

NG9-1-1 will facilitate the dynamic routing of emergency service requests to alternate ECCs based on a variety of factors. For example, ECCs could establish an overflow condition in which a maximum capacity of requests has been reached, a wait time threshold for answer or hold has been met, or during an outage or damage to an ECC's operational capability.

Evaluating ESInet Deployments

As mentioned earlier, state and local 9-1-1 authorities are procuring and implementing precursor technologies to modernize 9-1-1. These primarily consist of ESInets – individual IP-based networks that are intended to make ECCs ready to accept digital, IP-based inputs from originating service providers, connect ECCs to each other, and provide new levels of redundancy and resiliency. However, as experience has shown, ESInets are being deployed in a proprietary manner which causes them to lack interoperability (among ESInets and even between ESInets and CPE). Not only does this negatively impact operations, it also requires additional spending and resources to implement after-the-fact integrations and even more proprietary interfaces. Further, ESInets can be limited to supporting voice-based requests for emergency assistance and basic texts, which means enhancements for multimedia will be a separate, future cost item with another potential impediment to interoperability.

> In an end-state NG9-1-1 environment, callers in need of emergency assistance should not have to answer the same questions multiple times because PSTs cannot seamlessly transfer calls with incident data.

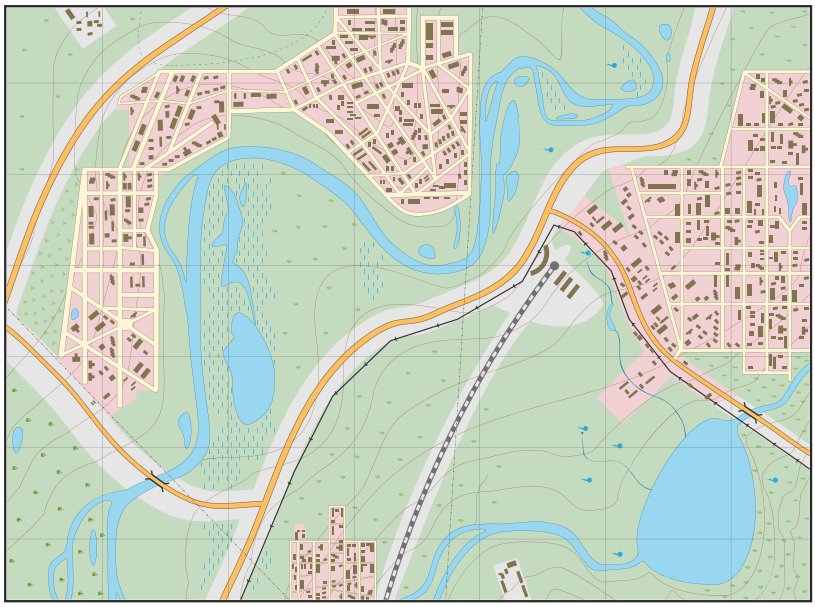
The 9-1-1 community deserves and demands better. ECCs have been saddled with interoperability problems in legacy networks,[3] and after spending hundreds of millions of dollars on ESInets, they should not have to experience the same problems.

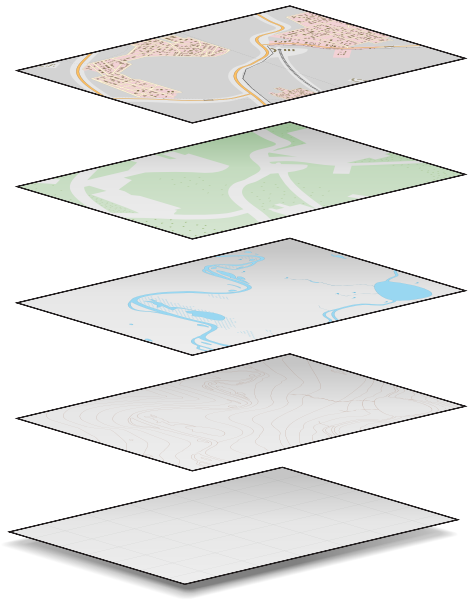
In an end-state NG9-1-1 environment, callers in need of emergency assistance should not have to answer the same questions multiple times because PSTs cannot seamlessly transfer calls with incident data. Further, the tools available to PSTs should be consistent, not a patchwork of haves and have-nots across the country.

When NG9-1-1 was first being contemplated, it was mostly understood to mean that ESInets would be deployed to support IP-based calls to ECCs. This limited vision of NG9-1-1 has led to multiple problems. First, focusing only on the call-delivery portion means missing the benefits of necessary enhancements to CAD and dispatch functions. This fragmentation invites interoperability problems, which means ECCs deal with additional proprietary solutions, costs, and delays when marrying the two portions together. Second, a piecemeal approach is and will be especially costly. Compounding the cost to overcome interoperability problems, ECCs may contend with redundant equipment purchases, abandoned investments, failed contracts, and equipment obsolescence before achieving fully interoperable and multimedia-capable NG9-1-1. Third, proceeding in stages introduces significant delays in achieving a full NG9-1-1 solution, thus stretching out the period when ECCs would have to maintain both legacy and NG9-1-1 systems. It also forces the continued reliance on legacy 9-1 1 transport and routing systems, removing incentives for originating service providers to deliver requests for emergency assistance in an IP-based format to 9-1-1. Fourth, the ongoing costs to maintain these legacy systems, in tandem with expenses related to ESInet development, negatively impact the ability of ECCs to fully fund additional progress through the remaining stages. Fifth, introducing IP-based elements without deploying a complete NG9-1-1 ecosystem adds new cybersecurity vulnerabilities. It would be much more efficient and effective to devise and implement a cybersecurity framework across an entire NG9-1-1 platform.

GIS Improvements

Mapping displays are a fundamental element of effective public safety emergency response. Geographic information systems (GIS) are the data management tools behind map displays, and





these systems have a significant role in organizing the advanced data and services coming with NG9-1-1. GIS will be integral to operationalizing locations of 9-1-1 callers and field responders, along with other relevant data that will significantly aid situational awareness.

Many states and jurisdictions have made significant strides in creating accurate GIS platforms and map layers, thus migrating from existing paper-based and more rudimentary maps. Caller location information and routing supplied by wireless service providers (including eventually dispatchable location) can be quickly integrated into GIS. A common misconception is that NG9-1-1 (or even ESInets in isolation) will improve 9-1-1 location information. In fact, wireless carriers are and will continue to be responsible for determining the caller's location and routing the call to the appropriate ECC. Improvements to location accuracy are separate from NG9-1-1. GIS, particularly in an NG9-1-1 environment, will enable ECCs to do more with the location information and other data they possess. Further, because emergency incidents go beyond the geographic boundaries of the originating community and public safety agencies routinely provide mutual aid, GIS must be part of the interoperability vision for NG9-1-1 more broadly.

The Role of Technology and Standards

Standards in the communications industry have led to the significant success that the public experiences with a vibrantly competitive marketplace, constant leaps in technology, and interoperability. These standards, developed by organizations including 3GPP, the Internet Engineering Task Force (IETF), and the Alliance for Telecommunications Industry Solutions (ATIS), ensure the public can share text, video, photos, and voice in an interoperable manner and regardless of the device or network. FirstNet and other public safety mobile broadband service providers also utilize commercial standards to drive significant economies of scale and ensure those first responders enjoy diverse features and device options.

NENA has developed an ANSI-approved specification for system architecture, commonly referred to as i3.[4] An i3-based system provides for the delivery of emergency calls through an IP-based network utilizing SIP.[5] By its very nature, i3 does not describe a complete NG9-1-1 system. There exists no current conformance program for i3. Yet vendors market solutions as "i3 compliant," including ESInets and related functional elements, which are not interoperable, lack multimedia capabilities, and often require costly proprietary interfaces and after-the-fact integrations.

Data and information generated through emergency requests for service must also be distributed in a standardized data structure. The joint APCO/NENA Emergency Incident Data Document (EIDD)[6] provides a standardized way to exchange emergency incident data between ECCs that may have different systems.[7] NENA subsequently devised the Emergency Incident Data Object (EIDO) Standard.[8] Solutions using EIDO, EIDD, or other standards must ensure that existing ways to format, store, and transmit data remain supported while extending support to newer formats.

The technology that will support the deployment of the NG9-1-1 system of the future will likely consist of cloud-based and hosted solutions, as well as system/software-as-a-service (SAAS) approaches. Precursors to NG9-1-1, such as ESInet deployments and OTT innovations delivering enhanced location information and new forms of data, are or may become integrated into these or newer technologies yet to be developed. Fundamentally, however, it is instructive to consider the role of technology and standards at a high level. The networks serving NG9-1-1 callers, other inputs to ECCs, and first responders in the field are sometimes the same network, and when they are different, interoperability is possible thanks to commercial standards deployed worldwide that have achieved remarkable levels of innovation. Now consider the NG9-1-1 systems in the center of these inputs/outputs. There should be no barriers that would make the ECC incompatible with the technologies and standards supporting the inputs and outputs. No proprietary interfaces. In fact, NG9-1-1 should essentially be based on the same standards and market forces that drive the networks supporting the callers in need and the first responders.

> NG9-1-1 should essentially be based on the same standards and market forces that drive the networks supporting the callers in need and the first responders.

To the maximum extent possible, 9-1-1 professionals should have the same operational experience regardless of their jurisdiction, and the public should similarly have available a common experience and expectation for how they access NG9-1-1 services, which has been historically the case for 9-1-1.

> The largest public safety organizations in the United States believe that achieving a nationwide upgrade to Next Generation 9-1-1 is possible by fully funding it through a federal grant program.

Getting On The Right Path

There are opportunities for 9-1-1 authorities and ECCs to move beyond the status quo of limited, staggered deployments that lack interoperability. Incentives are needed to influence and expand the NG9-1-1 vendor community to deliver on public safety's requirements. Additionally, requests for proposals should pursue complete, end-to-end solutions that are objectives-based toward achieving interoperability and other key requirements. This would lead to more integrated and efficient procurements and help ECCs more rapidly begin to match the public's expectations. The largest public safety organizations in the United States believe that achieving a nationwide upgrade to Next Generation 9-1-1 is possible by fully funding it through a federal grant program.[9] The goal would be to tie the achievement of key requirements to grant conditions.

Needed Capabilities

NG9-1-1 systems must be designed to be highly available and resilient. The public and field responders need to be able to expect that when help is needed, the ECC is continually operating and available to handle the request. In the event of disasters, or even during maintenance and updating of network, hardware, and software services, NG9-1-1 must be designed with geographically diverse logical and physical pathways and

systems to ensure no reduction in call handling effectiveness, with failover and self-recovery components. Network solutions, including for diversity paths, must also provide adequate bandwidth, availability, and speed to support access to multimedia and other data, and account for surges and expected growth in data. Using fiber, mobile broadband (such as FirstNet's nationwide public safety broadband network), cloud architecture, and, where necessary, satellites will provide additional network connectivity to the ECC for primary, backup, and remote operations.

Data analytics is the broad field of statistical processing of data that when applied to NG9-1-1 can help the ECC draw out meaningful, actionable information to assist the PST in identifying the most appropriate resources for any emergency service request.

With NG9-1-1 comes significantly more data, including multimedia, and thus the need for PSTs to access real-time and archived data through a multimedia, IP-based recording solution. Further, many states and local communities have established retention schedules for emergency call data extending the length of time records must be saved. A data recording solution in the NG9-1-1 environment must be capable of retaining all this new data. It must permit NG9-1-1 professionals to retrieve information needed to recreate an event in a time-synchronized manner or for other purposes such as sharing audio and video files with field-based responders during an incident or as an after-incident investigative tool.

Due to the vast amount of additional information that recording systems in an NG9-1-1 environment will need to store, solutions will likely take the form of cloud-based options rather than onsite equipment. Records should have physical security and be geo-diverse. Further, the data should be redactable and subject to strong cybersecurity and encryption techniques.

Data Analytics

Data analytics is the broad field of statistical processing of data that when applied to NG9-1-1 can help the ECC draw out meaningful, actionable information to assist the PST in identifying the most appropriate resources for any emergency service request. Analytics can also provide 9-1-1 professionals with trending data that can flag potential problems and present new insights. Data analytics is a continuous collection process that highlights when vital information is missing or incomplete and helps reduce data bias that would not otherwise be detectable.

ECC staff should have automated systems that can take advantage of large data sets to provide new insights for faster decision-making.

Significant information can be drawn from data through different analysis methods, whether in real-time or when reviewing historical data. This can come in handy in an NG9-1-1 environment where much more data is made available while PSTs cope with the need to perform quick analysis to ensure effective response and ongoing situational awareness and perform after-action review and event recreation. Post-event, these tools can offer descriptive analytics, such as a statistical measure of emergency call requests and the number of dispatched calls for service

during a specific time frame. Data analytics can also provide answers to why outcomes occur. For example, when an increase in transferred 9-1-1 calls occurs, an analysis might identify specific errors in the call routing system. Providing trends and predictions can help the ECC with operational needs such as staff scheduling changes during predicted high usage time periods. ECC staff should have automated systems that can take advantage of large data sets to provide new insights for faster decision-making. The inclusion of AI into data analytics can assist in prescriptive data analysis, which combines the outcomes from previous incidents to guide a current course of action.

Chapter 2

KEY TAKEAWAYS

- NG9-1-1 has the potential to provide the ECC with more types of data that will **empower PSTs to better serve the public and field responders**.
- NG9-1-1 systems can enable ECCs to **improve resilience and redundancy**.
- **ECCs should pursue end-to-end interoperable solutions**, avoiding proprietary approaches to NG9-1-1.
- **Data analytics can provide a new understanding** of public safety responses.

---

2 Public Safety Next Generation 9-1-1 Coalition http://www.ng-911coalition.org

3 CSRIC, (2020). *CSRIC VII Report on the Current State of Interoperability in the Nation's 911 Systems*. https://www.fcc.gov/file/18394/download

4 NENA, (2021). *NENA i3 Standard for Next Generation 9-1-1* (NENA-STA-010.3b-2021). https://www.nena.org/resource/resmgr/standards/nena-sta-010.3b-2021_i3_stan.pdf

5 Voice, messaging, video, and other communications applications over IP networks are accomplished with Session Initiation Protocol (SIP), a common communications standard. Setting up VoIP calls requires using SIP protocols; mobile telephone calls rely on SIP protocols for their VoIP services. Importantly for public safety, SIP communications can utilize encryption for enhanced security and protection from eavesdropping. See IETF, (2002). *SIP: Session Initiation Protocol*. https://datatracker.ietf.org/doc/html/rfc3261

6 APCO/NENA 2.105.1-2017

7 APCO, (2019). *Public Safety Communications Common Incident Types for Data Exchange* (APCO ANSI 2.103.2-2019). https://www.apcointl.org/~documents/standard/21032-2019-common-incident-type-for-data-exchange/?layout=default

8 NENA, (2021). *Emergency Incident Data Object EIDO* (NENA-STA-021.1a-2021). https://www.nena.org/resource/resmgr/standards/nena-sta-021.1a_eido_json_20.pdf

9 Public Safety Next Generation 9-1-1 Coalition http://www.ng-911coalition.org

Chapter 3
Fundamental Definitions and Principles

State definitions and requirements for NG9-1-1 vary significantly. Some definitions only include partial aspects of NG9-1-1, such as the ability of ECCs to receive IP-based calls and data, but do not incorporate a comprehensive end-to-end vision of NG9-1-1 that ensures ECCs have the tools needed to receive, process, store, and share multimedia information.

The lack of a universal, comprehensive, end-to-end definition creates confusion, makes managing public expectations more difficult, and creates a barrier to the nationwide deployment of NG9-1-1.

Similarly, states may inadvertently limit innovation in the NG9-1-1 environment by defining NG9-1-1 in a way that prescribes one particular standard or technology to be used. For example, several states define NG9-1-1 to mean 9-1-1 service that conforms to NENA's i3 standards. This approach can be detrimental because it is too narrow. NENA's i3 focuses on architectural elements and processes rather than required operational capabilities and is limited to call delivery and handling, thereby leaving unaddressed what capabilities a complete NG9-1-1 system must provide. This leads to some jurisdictions equating ESInet deployments and other i3-branded elements as constituting "NG9-1-1." In contrast, some states, have adopted a flexible definition that describes an operational capability and is closer to a comprehensive description.[10] Yet other states do not define NG9-1-1 in legislation at all.

The lack of a universal, comprehensive, end-to-end definition creates confusion, makes managing public expectations more difficult, and creates a barrier to the nationwide deployment of NG9-1-1. Recommendations for a comprehensive definition of NG9-1-1 are discussed further in this section.

Adopt Modern Definitions of NG9-1-1 and Other Key Terms

One of the fundamental steps in achieving NG9-1-1 is adopting modern definitions of key terms. Definitions, whether in laws or regulations, should align with public safety principles, requirements, and objectives. The following definitions have been included in federal legislative proposals that were crafted and supported by the public safety community.

Next Generation 9-1-1

An interoperable, secure, IP-based system that –

A. employs commonly accepted standards;

B. enables emergency communications centers to receive, process, and analyze all types of 9-1-1 requests for emergency assistance;

C. acquires and integrates additional information useful to handling 9-1-1 requests for emergency assistance; and

D. supports sharing information related to 9-1-1 requests for emergency assistance among emergency communications centers and emergency response providers.

9-1-1 Request for Emergency Assistance

A communication, such as voice, text, picture, multimedia, or any other type of data that is sent to a facility for the purpose of requesting emergency assistance.

Commonly Accepted Standards

The technical standards followed by the communications industry for network, device, and IP connectivity that –

A. enable interoperability; and

B. are –

1. developed and approved by a standards development organization that is accredited by an American or international standards body (such as the American National Standards Institute) in a process –

   i. that is open to the public, including open for participation by any person; and

   ii. provides for a conflict resolution process;

2. subject to an open comment and input process before being finalized by the standards development organization;

3. consensus-based; and

4. made publicly available once approved.

Emergency Communications Center

A facility that –

A. is designated to receive a 9-1-1 request for emergency assistance; and

B. performs one or more of the following functions –

1. process and analyze 9-1-1 requests for emergency assistance and information and data related to such requests;

2. dispatch appropriate emergency response providers;

3. transfer or exchange 9-1-1 requests for emergency assistance and information and data related to such requests with one or more facilities described in this paragraph and emergency response providers;

4. analyze any communications received from emergency response providers; and

5. support incident command functions; or

C. may be a public safety answering point, as defined in section 222 of the Communications Act of 1934 (47 U.S.C. 222).

Interoperability

The capability of emergency communications centers to receive 9–1–1 requests for emergency assistance and information/data related to such requests, such as location information and callback numbers from a person initiating the request, then process and share the 9–1–1 requests for emergency assistance and information/data related to such requests with other emergency communications centers and emergency response providers without the need for proprietary interfaces and regardless of jurisdiction, equipment, device, software, service provider, or other relevant factors.

Reliability

The employment of sufficient measures to ensure the ongoing operation of NG9-1-1 including using geo-diverse, device- and network-agnostic elements that provide more than one physical route between end points with no common points where a single failure at that point would cause all to fail.

State laws should include funding mechanisms that are sufficient for operational, capital, maintenance, and upgrade expenditures to support NG9-1-1.

Funding

A sufficient and enforceable funding mechanism is especially important to sustain an NG9-1-1 system and to promote the adoption of IP-based, broadband technology in ECCs. While states have a variety of 9-1-1 funding mechanisms in place, they might be limited to operational expenses, and not account for the combined costs of continued operations, maintenance, and technology upgrades. For example, according to the Federal Communications Commission's (FCC) thirteenth annual report on the collection and distribution of 9-1-1 and enhanced 9-1-1 (E9-1-1) fees and charges by the states, some states reported that their funding mechanism does not allow for the use of 9-1-1 funds for NG9-1-1 implementation.[11] State laws should include funding mechanisms that are sufficient for operational, capital, maintenance, and upgrade expenditures to support NG9-1-1.

Privacy

With NG9-1-1, the transmission and storage of data from a growing number of sources have implications for open records laws, citizens' privacy concerns, evidence authentication and chain of custody obligations, and data breach disclosure requirements. States and individual ECCs may need to amend their laws and policies so that they are suitable for an NG9-1-1 environment. For example, the application of open records laws largely depends on the definition of what constitutes a "record" kept by agencies in the course of conducting government business, and the new types of data in NG9-1-1 may expand the scope of what a "record" is. To illustrate this point, consider that Maine updated its confidentiality of system information law addressing personally identifiable information to include "any information that directly or by reasonable inference might disclose the identity of or personal information about a specific person or persons."[12]

Liability Protection

Liability protection can encourage private companies to innovate and serve the 9-1-1 community. Importantly, federal laws granting liability protections to 9-1-1 service providers are dependent on the liability protections offered in state law. Some states have modernized their 9-1-1 legislation to explicitly extend liability protection beyond legacy service providers to voice over IP (VoIP) and NG9-1-1 providers. For example, in enacting a law to require ECCs to implement NG9-1-1, North Carolina amended the liability protections covering service providers

to extend beyond voice service providers and include NG9-1-1 services.[13] Similarly, Tennessee law defines "non-wireline service" to include both wireless service and IP-enabled service providers, which enables equivalent liability protection to an IP-enabled service that offers 9-1-1 or E9-1-1.[14] Liability protections can address issues ranging from those related to 9-1-1 systems and services to the disclosure or release of subscriber information.

Delivery of Emergency Text Messaging Services

Text-to-911

The use of text-to-911 provides the ECC with the capability of turn-based messaging. FCC rules require all wireless carriers and certain other providers of text messaging applications in the United States to deliver emergency texts to ECCs that request the delivery of texts to 9-1-1. The FCC's text-to-911 rules do not apply to text messaging applications that do not support texting to and from U.S. phone numbers, nor do the rules require support for multimedia messages to 9-1-1.[15]

Real-time Text (RTT)

RTT is a text-based mode of communication where each text character appears on the receiving device at roughly the same time it is typed on the sending device, allowing for a conversational flow of communication. With RTT, a person on a call does not need to press "send" for the text to reach the other party. RTT uses IP technology to deliver texts. This is the same technology that supports VoIP. This technology also allows text and voice to be transmitted simultaneously during an RTT session.

> If requested by an ECC, a wireless carrier must begin delivering RTT communications in an RTT format within six months of the request.

When preparing to deploy RTT in the ECC, the wireless carriers that implement RTT are required to support RTT "calls" to 9-1-1. If requested by an ECC, a wireless carrier must begin delivering RTT communications in an RTT format within six months of the request.

Where a wireless carrier delivers RTT 9-1-1 calls to a legacy ECC served by a selective router, the wireless carrier is responsible for converting the calls to TTY before delivering the calls to the selective router. For RTT 9-1-1 calls to a legacy ECC served by an ESInet, the conversion to TTY is the responsibility of the ESInet provider.[16]

Integration of the Nationwide Public Safety Broadband Network Into the ECC

Understanding FirstNet and Its Relationship to NG9-1-1

The First Responder Network Authority (FirstNet Authority) is an independent authority within the U.S. Department of Commerce created by the Middle-Class Tax Relief and Job Creation Act.[17] The organization's mission is to develop, build, and operate a nationwide broadband network for first responders. The nationwide public safety broadband network (NPSBN), commonly referred to as FirstNet, is a public/private federal program that provides wireless broadband network for first responders. FirstNet is required to promote integration of the network with ECCs.[18]

Chapter 3

KEY TAKEAWAYS

- **ECC should adopt modern definitions** of key terms like NG9-1-1 and interoperability.
- **State laws may need to be revised to account for new privacy and liability concerns** in an NG9-1-1 environment.

[10] See, for example, KY. REV. STAT. ANN. § 65.7621(17) (2016) (defining NG9-1-1 as "a 9-1-1 system where any device capable of making a 9-1-1 emergency request uses digital technology through managed emergency services Internet protocol networks composed of functional elements and databases that replicate enhanced 9-1-1 features and functions while providing additional multimedia capabilities for the [ECC].").

[11] Thirteenth Annual Report to Congress on State Collection and Distribution of 911 and Enhanced 911 Fees and Charges, PS Docket No. 09-14, para. 56 (Dec. 31, 2021) available at https://www.fcc.gov/sites/default/files/13th-annual-911-fee-report-2021.pdf.

[12] ME. REV. STAT. TIT. 25, § 2929 (2015).

[13] N.C. GEN. STAT. § 143B-1413 (2015).

[14] TENN. CODE ANN. § 7-86-103(11) (2019).

[15] See Text to 911: *What You Need to Know*, Federal Communications Commission (last updated Jan. 6, 2020) https://www.fcc.gov/consumers/guides/what-you-need-know-about-text-911#:~:text=FCC%20rules%20require%20all%20wireless,that%20area%20within%20six%20months.

[16] See *Real-Time Text*, Federal Communications Commission (last updated Apr. 21, 2022) https://www.fcc.gov/real-time-text.

[17] See *Public Safety*, National Telecommunications and Information Administration (last updated Apr. 12, 2022) https://www.ntia.doc.gov/category/public-safety; see also Middle Class Tax Relief and Job Creation Act, Pub. L. 112-96, § 6204 (2012) (codified at 47 U.S.C. § 1424).

[18] Middle Class Tax Relief and Job Creation Act, Pub. L. 112-96, § 6206(b)(2)(C).

Chapter 4
Project Management & Lifecycle Planning

Implementing NG9-1-1 requires significant project management to ensure success and fulfill the vision of end-to-end NG9-1-1. ECC directors will need to define the project goals and work with various stakeholders to develop the project steps, including planning, execution, and project closeout. This is vital to avoid misalignment with ECC expectations or misinterpretations of performance requirements with vendors, consultants, and other contracted services. Project management is not just about implementing a technological solution within the ECC, but also ensuring that PSTs have the resources necessary to perform their lifesaving work.

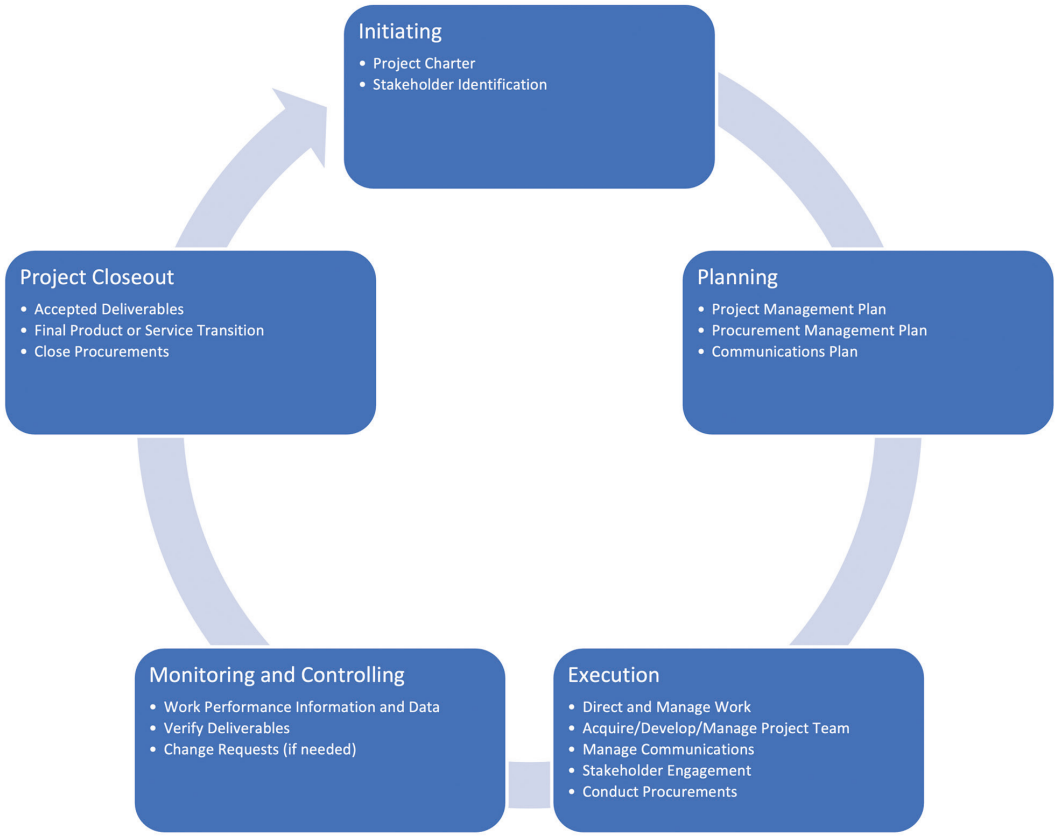
ECC directors should use project management best practices and methodologies when deploying NG9-1-1 to ensure more effective planning, procurement, and implementation of NG9-1-1 hardware, software, and services. Project management provides the following advantages to the ECC director:

- Development of clear and organized plans
- Clear definitions for stakeholder roles
- Well-outlined goals and objectives
- Increased sponsor and stakeholder buy-in
- Enhanced communications
- Efficient project completion

Project Management Methodology

The project management lifecycle can be broken down into five phases: initiating, planning, execution, monitoring and controlling, and closeout. Figure 1 provides an overview of these phases.

Figure 1: Project Management Lifecycle Overview



Project Initiating Phase

The project initiation phase sets the outline for the project by identifying a project sponsor and completing and authorizing the project charter. For most projects within an ECC, the project sponsor will be the senior manager that provides resources, support, and leadership to the project team, such as the ECC director or agency head. The project charter sets the parameters for the project and includes a statement of work (SOW) describing the business needs and a cost-benefit analysis for project justification. Each project charter should also have the following items:

- Project title
- Identified project manager (including authorization for the project manager to assign and use resources)
- Broadly written requirements
- Project purpose and justification
- Project description
- High-level risks
- Milestone schedule
- Budget
- Signature and approval by the project sponsor

In this phase, it is essential to describe your agency's goals and objectives for NG9-1-1. This ensures that the project team (e.g., ECC, vendors, and local stakeholders) understands how the project will enhance ECC operations. The project charter will also serve as a reference document to ensure the project remains within its original scope.

Project Planning Phase

Proper planning will directly impact project execution, and it is important to spend adequate time mapping out the project activities. While some project changes may be unavoidable, sufficient project planning will minimize the costs associated with unanticipated changes.

The project team will develop the project management plan (PMP) during the planning phase. The PMP will outline the following topics:

- Communications management plan
- Procurement management plan
- Activities to be completed (including the sequence of activities and estimated resources and duration)
- Project schedule
- Risk register (including identification of risks, qualitative and quantitative risk analysis, and plan for risk responses)
- Estimated costs
- Identification of key stakeholders and plan for human resources

It is essential to ensure that a jurisdictional representative is a member of the stakeholder group to help the project team navigate these processes.

For an NG9-1-1 implementation, some of these areas will be defined by jurisdictional regulations. For example, jurisdictions typically have a procurement management plan that project managers must follow. This could include RFP requirements, bidding procedures, or spending planning. It is essential to ensure that a jurisdictional representative is a member of the stakeholder group to help the project team navigate these processes.

Request for Information and Request for Proposal

In the project planning phase, ECC directors should develop a request for information (RFI) and a request for proposal (RFP) to aid in selecting vendors and developing the project scope. An RFI is a non-binding process that provides the ECC director with an understanding of the specific technology solutions and operational capabilities that may be available. This step will help identify prospective vendor solutions and services and offer clarification of marketplace solutions available

within the ECC service area. During this process, it is beneficial to include as many NG9-1-1 project team members as possible, including subject matter experts (SMEs) in operations, technology, finance, and purchasing and compliance.

During this process, it is beneficial to include as many NG9-1-1 project team members as possible, including subject matter experts (SMEs) in operations, technology, finance, and purchasing and compliance.

The RFI responses may also assist the ECC director with developing a formal RFP. Many RFPs are prepared from outdated, boilerplate language. This has hindered opportunities for increased competition and innovation. Specifically:

- ECCs are not getting the "next-gen" capabilities they expect because:
  - There is confusion about what "NG9-1-1" even means. "NG9-1-1" is not defined consistently and often not in a comprehensive way.
  - ECCs generally rely on cookie-cutter RFP templates developed by the industry rather than telling solution providers what is needed.
  - Interoperability is either left to be worked out after the fact or not addressed at all. ESInets from different vendors might not be able to transfer calls, and call handling CPE might not be able to receive calls from another vendor's ESInet.

- Cybersecurity, which is especially important for IP-based networks, is not being given enough attention in current RFP templates.

- States or localities act in silos to procure products and services from a limited pool of vendors.
  - The 9-1-1 community represents a small customer base with relatively low bargaining power. Accordingly, vendors do not have the same incentives to innovate, compete, or provide interoperable, non-proprietary solutions to the degree enjoyed by consumers in the greater commercial marketplace.
  - New companies with fresh thinking who incorporate modern communications technologies are gaining some ground. Still, they must compete with the traditional way of doing business that often does not serve the best interests of ECCs.

- Most RFPs are limited to "ESInets" or "next-gen core services," while others include only data offerings (i.e., CAD, RMS, mobile data, etc.). A comprehensive approach is more likely to result in interoperability and cost-efficiencies. Yet even if NG9-1-1 is pursued in stages, RFPs need to clarify the expected end-state solution to avoid overly complicated and costly future integrations.

APCO's RFP Template is comprehensive in nature to cover all aspects of a complete NG9-1-1 deployment, regardless of the stage any state or locality is in concerning the transition to NG9-1-1.

APCO prepared a "Sample RFP Template for NG9-1-1 Capabilities"[19], found on page 57, to assist 9-1-1 directors and authorities with their procurement activities, whether for a statewide or local effort. This document is a first of its kind from APCO and is intended to address several concerns APCO has identified with the state of progress toward NG9-1-1.

APCO's RFP Template is comprehensive in nature to cover all aspects of a complete NG9-1-1 deployment, regardless of the stage any state or locality is in concerning the transition to NG9-1-1. The RFP Template offers recommendations, guidance, and specific operational requirements that will interest any state or local official involved in the procurement process, especially state-level 9-1-1 officials as well as directors and managers of ECCs.

Consulting Services

While it may be beneficial to use consulting services when developing RFI and RFP documents, the ECC director must still ensure that the documents reflect the specific needs of the ECC and its service area and do not simply offer a general solution. ECC directors should be fully involved with the consulting services to avoid misinterpreting performance requirements. Similarly, ECC directors should ensure that consulting services directly engage with stakeholders involved in the project. Full involvement by all participating stakeholders will ensure the RFP produced represents a thorough understanding of the service capabilities of the ECC.

Evaluation

Before evaluating any RFP response, a jurisdiction must fully develop its requirements for an NG9-1-1 system. Once requirements are set, they should be categorized into "wants" and "needs" with a higher value given to requirements in the needs category. If a vendor cannot meet the "needs" category during the RFP process, the proposal should be rejected. To eliminate any confusion, vendors should not be allowed to participate in the RFP development process. Additionally, the project manager should develop a scoring matrix to evaluate the hardware, software, services, and capabilities of the proposed NG9-1-1 solution. The scoring matrix should provide a weighted scoring system for the project manager to rank the importance of each RFP requirement relative to how vital that provision may be to the project's overall success.

While projects are often awarded to the lowest bid, on complex projects such as NG9-1-1, the need for critical infrastructure and premise-based equipment should be considered, and preference should be given to technical solutions that favor reliability and interoperability over lower cost. To ensure transparency and fairness during the evaluation process, project team members should be provided with a formal process to ask clarifying questions, which should be shared with other bidders. Additionally, interviewing qualified bidders can provide clarification of the proposed solutions and an opportunity to introduce the vendor's project team members.

While projects are often awarded to the lowest bid, on complex projects such as NG9-1-1, the need for critical infrastructure and premise-based equipment should be considered, and preference should be given to technical solutions that favor reliability and interoperability over lower cost.

Finally, before awarding any bid for NG9-1-1, it is incumbent upon the ECC director to perform due diligence in reviewing past vendor performance, including interviewing former and current customers, examining the fiscal health of the vendor(s) and subcontractors, and evaluating if any recent acquisitions or mergers may reduce long term support for any product or solution provided.

When contacting former and current customers, it is essential to prepare a questionnaire that reflects the scope of work and project goals and includes questions related to the technical and operational requirements of the project, the level of customer service and responsiveness provided, the ability of the vendor(s) and its subcontractors (if any) to meet project timelines, and adherence to the change order procedure and the project budget.

Funding and Sustainment

For some time, ECC directors will be responsible for securing funding for NG9-1-1 projects while simultaneously supporting ongoing maintenance costs for legacy systems. Many state and local funding mechanisms for 9-1-1 do not adequately account for new services that offer emergency communications in an NG9-1-1 environment. ECC directors will need to ensure that financial and technical mechanisms are in place to sustain the existing systems and prepare for system replacement. ECC directors should develop a sustainable funding plan that includes:

- An audit of the current 9-1-1 system and its technological maturity (including predictions for eventual decline)
- A calculation of network and backhaul operating costs through the end of life (EOL) as well as ongoing operational expenses (OpEx), including utility costs, fees, and leases
- A project budget that distinctly identifies the separate costs associated with capital expenditure (CapEx) related to NG9-1-1 investments and those related to ongoing maintenance of legacy systems
- A plan for the continual refresh of hardware, software, and user equipment throughout the 9-1-1 system's technological maturity
- Establishment of payment milestones (to be incorporated into the project budget)

A sustainable funding plan will help ECC directors determine what sources of funding may be available and how much funding they need.[20] ECCs may be able to reduce costs by coordinating purchases with similarly situated ECCs and sharing equipment, networks, and software or hardware.

ECCs may be able to reduce costs by coordinating purchases with similarly situated ECCs and sharing equipment, networks, and software or hardware.

Project Execution Phase

Once a project has progressed past the initiating and planning phases, it is time to execute the project plan. In this phase, project managers will:

- Direct and manage work
- Acquire, develop, and manage the project team
- Manage communication (per the communications management plan)
- Conduct stakeholder engagement
- Conduct procurements

In accordance with the procurement management plan, project managers begin purchasing and acquiring necessary resources, including people, and facilitating stakeholder engagement.

Project Monitoring and Controlling

Once a project begins work, the project manager must monitor project performance and make changes to the PMP as needed based on work performance data and deliverable status. Some of the data monitored during this phase will include:

- Quality of work performance (including how work performance aligns with the project scope)
- Adherence to budget and overall costs
- Communications according to the communications management plan
- Risks encountered as compared to the risk register
- Procurements
- Adherence to the project schedule
- Stakeholder engagement

If alterations to the PMP are needed, the project manager will need to submit a change request to project sponsors. This document will outline the problem, what needs to change, and the impacts on cost and schedule. The project sponsor must

authorize any change requests in writing. If the project sponsor accepts the change request, the project manager can integrate the applicable changes into the project.

Project Closeout Phase

Although an often-forgotten phase, the project closeout is essential to ensuring success for future projects. This phase includes a formal meeting between the project sponsor, project manager, and all stakeholders to discuss which project activities were successful and which needed improvement. With the project closeout meeting information, jurisdictions can implement lessons learned for future NG9-1-1 implementations, upgrades, and fixes. In the emergency communications industry, this is often referred to as an after-action review (AAR).

ECC directors should also perform a complete inventory of hardware, software, and services that may no longer be needed when preparing for the decommissioning and disposal of assets during the final phases of the project.

At the end of this meeting, all project deliverables should be fully implemented, tested, and transitioned. Organizational assets should be updated to reflect the new NG9-1-1 equipment and integrated into the technology inventory and lifecycle planning. All procurements should be completely closed out (i.e., completed and paid). ECC directors should also perform a complete inventory of hardware, software, and services that may no longer be needed when preparing for the decommissioning and disposal of assets during the final phases of the project. Additional consideration of any regulatory requirement that may impact the disposal options, including potential new costs, must be determined. Accurate tracking throughout the lifecycle of resources includes the final disposal process and ensuring effective cyber hygiene to protect from possible data loss.

Chapter 4

KEY TAKEAWAYS

- **Project management methodologies can help focus the project scope**, minimize risk, and provide a roadmap for implementing the project in an efficient and cost-effective manner.
- Best practices can help **define technical and operational objectives and project steps** and assist in identifying stakeholders.
- Sufficient time and effort should be dedicated to **the project planning phase**.
- A request for information (RFI) may **provide a benefit in identifying NG9-1-1 solutions** not fully known to the ECC.
- A request for proposal (RFP) **requires specific operational and functional requirements** of the system to provide interoperable end-to-end capabilities.
- The project manager should **monitor key data points** on project implementation.
- The project closeout should include a plan for the **decommissioning and disposal of assets** no longer needed.
- **Ensuring adequate funding for Next Generation 9-1-1** is one of the most significant challenges to the ECC director.
- Preparing and implementing Next Generation 9-1-1 is the **first step in the technology ecosystem lifecycle process**.
- It is necessary to **plan for the continual refresh of hardware, software, and user equipment** throughout the system's technical maturity.

19 *Sample RFP Template for NG9-1-1 Capabilities*, APCO International (last visited June 21, 2022) available at https://www.apcointl.org/technology/next-generation-9-1-1/sample-rfp-template-for-ng9-1-1-capabilities/.

20 *Funding Mechanisms Guide for Public Safety Communications*, CISA (June 2021) available at https://www.cisa.gov/safecom/funding#.

Chapter 5

APCO's Sample RFP Template for NG9-1-1 Capabilities

APCO prepared the "Sample RFP Template for NG9-1-1 Capabilities" to assist 9-1-1 directors and authorities with their procurement activities, whether for a statewide or local effort. This document is a first of its kind from APCO and is intended to address several concerns APCO has identified with the state of progress toward NG9-1-1.

The RFP Template is comprehensive in nature to cover all aspects of a complete NG9-1-1 deployment, regardless of the stage any state or locality is in concerning the transition to NG9-1-1. The RFP Template offers recommendations, guidance, and specific operational requirements that will be of interest to any state or local official involved in the procurement process, especially state-level 9-1-1 officials and directors and managers of ECCs.

The full RFP can be found on page 57.
To access the RFP as an editable word document, visit apcointl.org/ng911rfp.


msnbc
NBC/MARIST POLLS: DEMS STAY COMPETITIVE
100% Your Own Hair
10:39
10:39:29

Chapter 6
Operational Impacts

As discussed in earlier chapters, NG9-1-1 will accelerate the amount of information ECCs and responding agencies receive. The receipt and processing of this new data will have substantial impacts on ECC operations. To ensure that both ECCs and PSTs are prepared, agencies must develop policies and procedures to address the new functions, interfaces, and information flows involved in NG9-1-1 operations and the related roles of individual personnel. 9-1-1 agencies will need to anticipate the expected amount and types of data the ECC would receive, and the personnel needed to process such data. Workload, call management, and psychological impact on the PST are significant issues to address. While NG9-1-1 will bring new opportunities to improve emergency response, ECCs will need to overcome the operational challenges that will follow.

Information Flows to the ECC

One of the most frequently mentioned benefits associated with NG9-1-1 is the ability for an individual to send real-time photos and videos of the emergency being reported. However, there are several additional types of data ECCs will be able to receive and share in an NG9-1-1 environment. Home medical devices and electronic health records can store and share patient information to assist with pre-hospital emergency treatment. Interfaces to numerous camera systems, including schools, critical infrastructure facilities, and public gathering places, can connect to provide real-time situational awareness. Officer-worn body cameras and security surveillance systems can be streamed directly to the ECCs to aid communications with field responders.

Multimedia-based requests and supplemental incident data must be analyzed and evaluated with the same critical assessment as traditional voice calls to validate data and information.[21] Inaccurate or incomplete data and information can reduce response capabilities and negatively affect incident outcomes. PSTs may be able to incorporate analytical systems developed with data mining, artificial intelligence, or cognitive abilities to triage the information and provide dispatch recommendations. One approach for processing this type of traffic is a "dashboard" on the call entry screen of the NG9-1-1 call processing equipment monitor. This dashboard could allow the PST to identify if there are photos, videos, or other data available which can be shared with responders in the field or accessed during follow-up investigations. Another element of the dashboard could inform the PST whether additional surveillance footage of the incident was available, such as imagery from traffic or security cameras (commercial and residential), drone video, "shots fired" information, etc.

Interfaces to numerous camera systems, including schools, critical infrastructure facilities, and public gathering places, can connect to provide real-time situational awareness.

Because call processing times can vary depending on the type of information being received, analyzing this influx of information is likely to be more time-consuming than call processing in a legacy environment where call processing times are more readily established and managed. Operations will need to adjust, measure, and manage call flows and processing times when additional data sources need to be triaged.

Information Flows Between ECCs and Emergency Responders

NG9-1-1 technology will make marked improvements in the ability and ease of transferring information between ECCs and responders in the field. ECC policies will need to

govern when and how to transfer a 9-1-1 call and associated data to ensure seamless operations and cover shifting responsibilities over the data, such as record management and liability. Not only will ECCs be capable of transferring CAD and 9-1-1 information to other ECCs, but they will also be capable of sending that information to multiple agencies, regardless of jurisdictional boundaries. When to transfer a call can, depending on the need to transfer, be a complex decision matrix. In most cases, policies, procedures, and protocols need to be put in place well in advance and trained on regularly so that information transfer is a seamless operation.

ECCs will also need to develop policies and procedures that consider sharing data and information with responders in the field, what information should be shared, and when that information should be shared. Many CAD systems handle the exchange of information from CAD to mobile data terminal/computer (MDT/C). As services continue to upgrade older CAD systems to current systems, access to information and storage has improved. However, issues still exist with archival data being available for immediate retrieval and true interoperability between systems. Policies and procedures will need to consider the transition period as IP connectivity and broadband technologies are introduced.

> Policies should address what types of information can or should be sent to field responders based on the role of the responder receiving the information.

In addition to determining how to share information, ECCs must decide what information should be shared. Policies should address what types of information can or should be sent to field responders based on the role of the responder receiving the information. For example, building records and floor plans sent through CAD to Incident Command will enhance responders' abilities to locate 9-1-1 callers. But not all responders in the field will need to receive all available information the PST may have at their disposal.

Impact to PSTs

Regardless of the technology available, PSTs will add value to the operations based on their training and skillsets. The operational impacts of NG9-1-1 implementation will drive new training and workforce requirements. The stress levels, work environments, expectations, and job conditions can overwhelm veteran staff members and newcomers. Developing strategies to address the impacts of NG9-1-1 on the ECC workforce will be critical. With increased NG9-1-1 data, ECCs will be expected to do more with the same staffing. In some instances, ECCs may need to hire additional staff with enhanced skillsets which will impact staffing and training budgets. ECC policies must account for new skillsets, potential new positions, and ECC personnel's mental health and wellbeing.

Need for New Skills and Positions

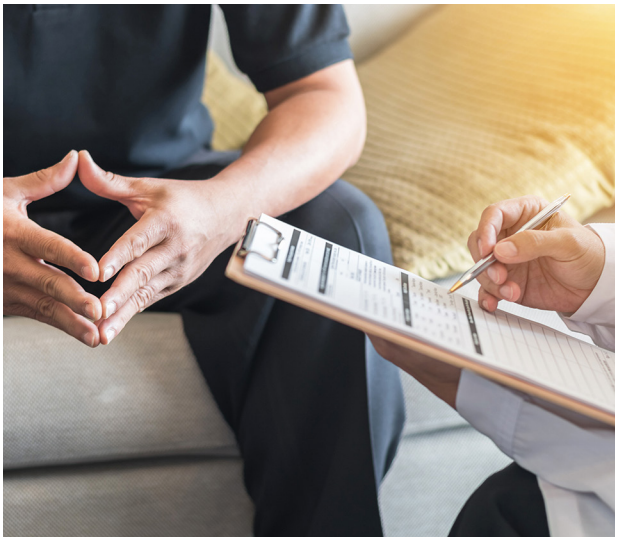
Many of the tasks performed and demonstrated by PSTs in an NG9-1-1 environment will be fundamentally the same as today. PSTs will still need important skills such as enhanced multitasking, critical thinking, strategic decision-making, problem identification, analytical analysis, etc. However, the variations in the types of data PSTs are exposed to and the new forms of technology available may require additional skillsets, as described further in the training section. ECCs will need staff that can expand on existing knowledge, skills, and abilities, including cybersecurity awareness, familiarity with digital, broadband, and IP-based technology, and the ability to sift through and prioritize increased volumes and data types.

Some aspects of NG9-1-1 may warrant the creation of entirely new positions within the ECC. ECCs need to account for new job functions either by hiring additional personnel or absorbing new requirements into existing positions. For example, to deal with multiple inflows of multimedia data, a dedicated position could serve as an analyst of inbound traffic and determine what multimedia data should be shared with responders in the field, which responders should receive the information, and in what format. Other staff positions could be dedicated solely to analyzing and processing surveillance imagery, monitoring and processing information from first responder sensors (such as biometric telemetry from firefighters or body cam footage from police officers), or liaising between the ECC and external entities who are managing this data on behalf of the ECC.

Some aspects of NG9-1-1 may warrant the creation of entirely new positions within the ECC.

Recruitment and Retention

The implementation of NG9-1-1 will require PSTs to take on additional roles and learn more about the technologies available to them. This environment may present new challenges in recruiting and retaining ECC personnel and exacerbate current staffing issues. Generational differences in the workforce will become more evident as recruitment and retention of tech-savvy personnel becomes more beneficial to aid with technological advancements. If an ECC is dealing with a staffing shortage, adding the challenge of adopting new technology could be more complex and even detrimental to operations. On the other hand, broadband technology can help ECCs with staffing shortages, for example, by creating connections to other ECCs for failover during high call volumes.



Impacts on Mental Health

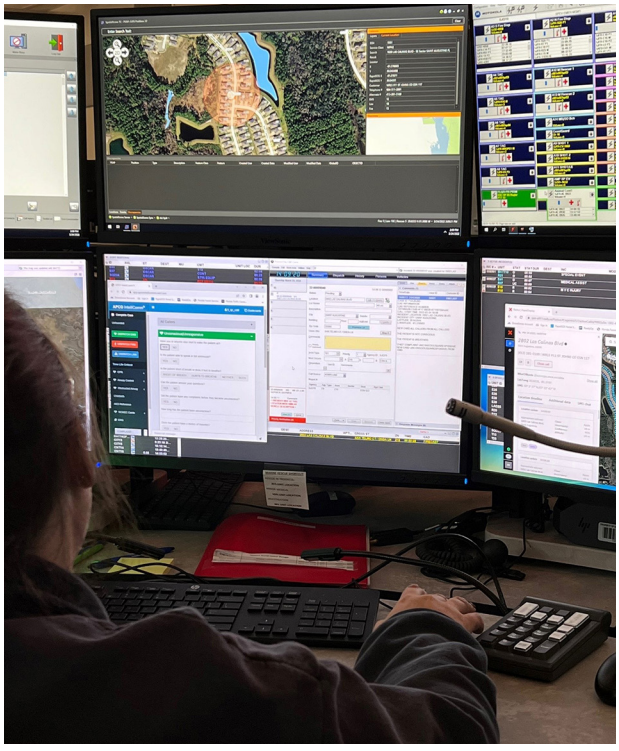
Today, PSTs face significant mental health impacts as part of their role in emergency response. In contrast to voice calls, incident-related photos and video messaging will have a different and more disturbing impact on PSTs and may lead to additional stress-induced issues. Because ECCs are the concentration point for incidents, the exposure to high volumes of information and disturbing content may be incredibly intense for staff. Further, the unique responsibilities of PSTs mean they

cannot necessarily take a break before responding to the next call for service from the public, processing new information from other agencies, or assisting first responders facing life-threatening situations. Preparing staff for this type of traffic and hiring the right personnel with appropriate skill sets is key.

Burnout considerations will be an increasing problem as the number of tasks required for PSTs increases, and job satisfaction and employee retention could likely decrease. ECCs will need to incorporate mental and emotional resiliency training for staff to handle the additional stressors. Similarly, ECCs should also implement systems for monitoring and addressing staff mental health needs, such as debriefing services, chaplains, employee assistance programs, department counselors, critical incident stress debriefings, and peer support programs.

New Training Needs

Training will be critical to preparing for and implementing NG9-1-1 technologies and services. PSTs are already trained in interpersonal communications skills involving voice communications. Still, in an NG9-1-1 environment, PSTs must be prepared to use this skill when communicating with callers via text message or video. In addition, PSTs will have more information at their disposal about the emergency being reported. PSTs will have to learn new multitasking skills, possibly using features embedded in the NG9-1-1 systems, to rapidly analyze more significant amounts of data. Learning to determine the value of live and recorded video, still images, and metadata for the assessment of situational awareness will require sufficient training for PSTs.



To fully take advantage of these advanced capabilities for the benefit of public safety, PSTs will need additional training. For example:

- How to incorporate live video from a caller or an agency-operated source into call processing and dispatching.
- How to manage PST support from a partner agency that may have different capabilities.
- How to incorporate more detailed patient information into an assessment as part of emergency medical dispatch.
- How to manage the increased stress that will come from exposure to images and increased operational involvement that has traditionally been limited to field responders.

> Additional training in the use of social media and other web-based services may help avoid the inclusion of deceptive or false information posted to confuse or redirect field-based responders or install malware/spyware on ECC networked systems.

PSTs will need training related to the components that make up NG9-1-1, including GIS tools that may provide the PST with more location information and cybersecurity protections that secure access to data, maintain the integrity of the data, and dispose appropriately of retired media. Additional training in the use of social media and other web-based

services may help avoid the inclusion of deceptive or false information posted to confuse or redirect field-based responders or install malware/spyware on ECC networked systems.

As the expectations of the public become increasingly disconnected from the actual capabilities of ECCs, public education programs will be necessary to provide useful information to the public as to the capabilities and limitations of ECC operations.

To facilitate improved training for ECC personnel in an NG9-1-1 environment, training standards should reflect the characteristics of the fast-paced nature of broadband technology. Training models and strategies will need to continually adapt, considering the generational differences of PSTs in the workforce. Consider, for example, a situational awareness app that provides live video feeds, real-time location tracking, and biometric data from field responders to the ECC. Today's newest PSTs may have grown up with smartphones and tablets, requiring minimal training on these devices. In contrast, older generations may be more unfamiliar with the advanced technologies and require more extensive training. The capacity for broadband technology to be widespread and intuitive to consumers can be leveraged to create model training programs for PSTs while preserving flexibility to meet requirements specific to varying workforce compositions.

Manage Public Expectations

Engagement between the public and the ECC should be encouraged. Still, rapid changes in technology available to consumers have contributed to misconceptions among the public about the technological capabilities of an ECC. A better-informed public can mitigate the impacts on operations from today's legacy systems through the transition and eventual completion of NG9-1-1. For example, public education campaigns for nascent text-to-911 services have successfully reinforced the concept to "call if you can, text if you can't." As the expectations of the public become increasingly disconnected from the actual capabilities of ECCs, public education programs will be necessary to provide useful information to the public as to the capabilities and limitations of ECC operations.

New Operational Policies

The current 9-1-1 environment supports a structured process with a relatively clear delineation of responsibilities defined by statutes, rules, and common practices. NG9-1-1 introduces complexities into this structure, requiring increased coordination and partnership among stakeholders, and may require a reexamination of existing governance and policy structures relating to all entities involved (dispatch, law enforcement, EMS, fire, emergency management, etc.).

Model policy development will include, but not be limited to, 9-1-1 call processing, CAD, GIS, GPS, ESInet, RMS, use of recording and retention systems, and dispatch console (radio) operations. This will require an evaluation of a variety of potential policy solutions and analysis of existing consensus-based standards and best practices. ECCs will need new standard operating procedures (SOPs) to ensure that the handling, dissemination, and storage of the information received is compliant with all local, county, state, and federal laws and regulations.

Modification to existing practices, procedures, and resources to accommodate NG9-1-1 must address, but not be limited to:

- Call taker expectations and responsibilities.
- Coordination across ECCs and other 9-1-1 authorities.
- Coordination across essential emergency service providers, application providers, and telecom providers.
- Service quality, cybersecurity, disaster recovery, and business continuity plans.
- Methods and procedures for new ECC hosted services such as CAD systems and medical record access.

Data Storage and Retention

The volume of data and diversity of data storage systems may present challenges when drafting after-action reviews, complying with court-mandated orders, or providing information to the public. Storage of data and records retention will be a significant concern, and local requirements for data retention will drive agency requirements for equipment or services and cannot be overlooked. In addition, with specific hosted solutions, the records may be retained in more than one place (this is recommended from a security perspective), and consideration must be given to the custodian of record requirements.

SOPs must ensure that handling, dissemination, and storage of received information complies with all local, state, and federal laws and regulations while maintaining an orderly and efficient data flow. This extends to tracking information flow and flagging information for confidentiality, evidentiary, chain of custody, and investigative purposes.

Quality Assurance

One of the more significant impacts of NG9-1-1 being introduced into the ECC is the impact on quality assurance. Not only will calls continue to require systematic and objective review, but new data types, requirements, capabilities, and stresses will all have to be considered.

The following are recommended updates to the QA program:

- Set clearly defined minimum standards and expectations for processing SMS/text-to-911 and multimedia/MMS calls. PSTs must understand the QA program.
- Create pre-scripted "interview" questions for each public safety discipline (police, fire, EMS).
- Set minimum expectations for gathering critical criteria (address, callback telephone number, nature of the emergency, etc.).
- Establish requirements for objective scoring categories and supporting standard evaluation guidelines (SEGs) (ex., below expectations, meets expectations, exceeds expectations, etc.).
- Maintain a log of all incoming SMS/text-to-911 and multimedia/MMS calls subject to random or requested/special review in the QA program.
- Access and print transcripts of SMS/text-to-911 and multimedia/MMS calls as needed along with other associated information (CAD event, ANI/ALI data, etc.).
- Review data, photos, videos, etc. associated with the incident (if applicable) to assess how the call taker used this information.
- Provide appropriate training for conducting reviews on SMS/text-to-911 and multimedia/MMS calls to QA evaluators.
- Establish timeline benchmarks for conducting QA reviews on SMS/text-to-911 calls (ex., weekly, monthly, etc.).
- Establish an accountability process, performance improvement plans, and corrective action specific to SMS/text-to-911 and multimedia/MMS calls as required.
- Establish a process for providing training and corrective action specific to SMS/text-to-911 calls, as necessary.
- Identify system trends through recording and tracking areas of excellence and those identified for improvement discovered in reviews so that this information can be used in future training (in-service training, remedial training, training bulletins, etc.).
- Implement or expand critical incident stress debriefing to address post traumatic stress disorder (PTSD) experienced by PSTs exposed to disturbing multimedia/MMS data.

Criteria-based electronic guidecards for medical, law enforcement, fire, and non-traditional responder requests for emergency assistance can help improve the end-to-end call flow by including relevant information delivered by NG9-1-1 and additionally provide QA evaluations to improve PST performance.[22]

Effective Processing Rather Than Facilitating Information Overload

Too much irrelevant data and information can increase processing time, introduce errors in the decision-making process, and delay response. New procedures must be developed, and additional

steps must be taken, to assess and evaluate disputed data and information to validate and resolve conflict. Data that can improve caller and field responder safety, provide additional information for medical care, and assist court proceedings must be separated from data that does not inform or is not material to the decision-making process.

Priorities must be given to information of an emergent nature; for example, crimes in progress, fires, and medical emergencies must be relayed immediately to dispatch. ECC policies should assign a staff member to interpret the incoming information, determine the priority, and send it to the appropriate service for dispatch. Eventually, this may be done within the system by a "keyword search" program. Still, ECCs may lose the opportunity to gain valuable information that only a trained PST can gather (EMD questions, suspect description, fire exposures, or entrapment data that can protect both callers and emergency responders).

Priorities must be given to information of an emergent nature; for example, crimes in progress, fires, and medical emergencies must be relayed immediately to dispatch.

Chapter 6

KEY TAKEAWAYS

- ECCs will need to make **operational changes to accommodate new types and amounts of data** received.
- Policies and procedures will need to be established for **how and when to share NG9-1-1 data with other ECCs** and responders in the field.
- ECCs may need to **enlist new personnel specifically responsible for analyzing and processing NG9-1-1-related data**.
- **ECC personnel will require additional forms of training** related to working with broadband technologies.
- SOPs will need to be altered to reflect **new concerns present in an NG9-1-1 environment**, such as data storage and quality assurance.

[21] APCO, (2018). *Core Competencies, Operational Factors, and Training for Next Generation Technologies in Public Safety Communications* (APCO ANS 1.115.1-2018). https://www.apcointl.org/~documents/standard/11151-2018-nextgen-technologies-in-public-safety-communications

[22] APCO, (2015). *Standards for the Establishment of a Quality Assurance and Quality Improvement Program for Public Safety Answering Points* (APCO/NENA ANS 1.107.1.2015). https://www.apcointl.org/~documents/standard/31062-2017-qae/?layout=default

Chapter 7
Security Considerations

The implementation of NG9-1-1 technology provides ECCs with the opportunity to take a holistic approach to cybersecurity protections. As APCO has previously stated, cybersecurity should be baked in, not bolted on.[23] This means cybersecurity protections should be incorporated by design into planning, implementation, and operation models from the onset. Viewing cybersecurity in this manner will reduce the need for costly, after-the-fact solutions that may not meet the level of security protections required by emergency communications. ECCs will need to ensure that their technical and operational cybersecurity protocols are sufficient for both an NG9-1-1 and a legacy environment.

New Threat Vectors for NG9-1-1

With the current E9-1-1 environment, there are challenges and threats that will continue to evolve and, without proper mitigation techniques, pose threats to ECCs. These challenges include spoofing, swatting, and hacking known vulnerabilities in systems, networks, and infrastructure. With the implementation of NG9-1-1, some of these challenges will be mitigated. However, new threats will arise as bad actors identify new tactics, techniques, and procedures (TTPs) to exploit emergency communications equipment. As ECCs transition to IP-based technologies, 9-1-1 systems will transition from operating on networks with limited access to sharing networks with other ECCs, agencies, and vendors. This open environment will create new ways to access emergency communications networks, thus further increasing the risk of a cyberattack.

Due to the critical nature of the work performed, ECCs will continue to be a high-value target for multiple categories of hackers. Despite the substantial risk of cyberattacks, many ECCs have inadequate protective infrastructure and lack appropriate and industry-specific cybersecurity training.

ECCs will need to ensure that their technical and operational cybersecurity protocols are sufficient for both an NG9-1-1 and a legacy environment.

Hardware and Software Vulnerabilities

NG9-1-1 implementation will require significant hardware and software upgrades to any ECC. From a cybersecurity perspective, some factors to consider for hardware cybersecurity are EOL support, maintenance, zero-day vulnerabilities, known threats, and flash updates.

EOL support can be critical as the emergency communications industry transitions from E9-1-1 to NG9-1-1. EOL support refers to the assistance a company offers after it decides to discontinue a product or service. For example, after Microsoft discontinued support for Windows 7 the company provided users an iterative path to upgrade their operating system before support would no longer be provided.

ECC stakeholders should understand how their hardware solutions will handle zero-day vulnerabilities, known threats, and flash updates. A zero-day vulnerability is a security flaw that has been disclosed and identified, but a mitigation patch has not been developed. Once a vulnerability is known, it is incorporated into the Known Exploited Vulnerabilities Catalog along with any known mitigation techniques.[24] Any cybersecurity plan should include a strategy to update and protect ECCs from zero-day and known vulnerabilities, such as through flash updates, regular security updates, or other mitigation strategies determined by local resources.

ECCs should examine any new pieces of hardware and software that will be installed on local networks. IT professionals should review the new pieces of equipment in a virtually secure and segmented environment where they can determine if a device has any known vulnerabilities already installed (known as a pre-hacked device). An IT Department should sanitize all hardware and software that will be incorporated into the ECC network to ensure it is safe.

Before selecting an NG9-1-1 solution vendor, ECCs should verify the following information:

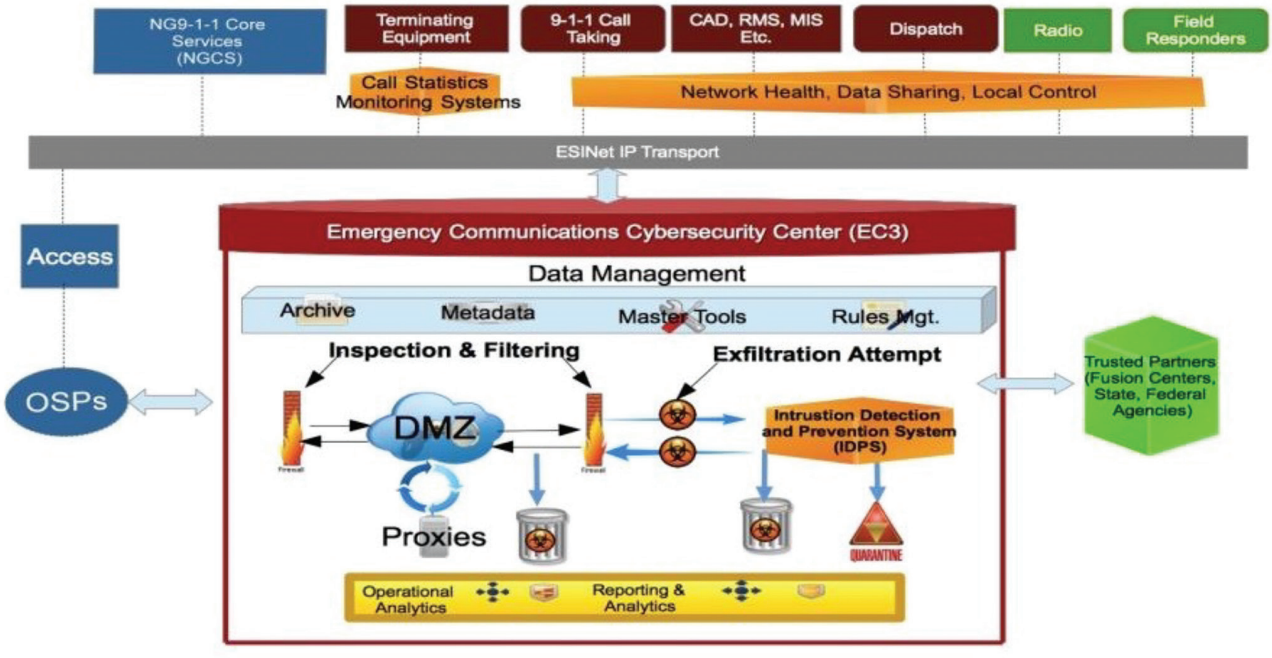
- How are security patches provided to the ECC? ECCs should work with software vendors to ensure that these security patches adhere to local policies and procedures and do not interrupt ongoing services.
- For regularly scheduled updates, how will the vendor work with local IT support to implement security patches? ECCs must be prepared for any system change and coordinate with IT staff.
- What is the EOL support plan? When a vendor stops support for a software program, local jurisdictions should understand what the EOL support plan will be.
- If there is a need for a version update, will there be any costs for the ECC and will the vendor outline the known cybersecurity vulnerabilities? Software evergreen is essential to address emerging cyber threats and to improve or add functionality to the ECC.

NG9-1-1 Cybersecurity Architecture Centralized

The FCC's Task Force on Optimal PSAP Architecture (TFOPA) reports outlined a cybersecurity defense mechanism called the Emergency Communications Cybersecurity Center (EC3) (see Figure 2).[25] The EC3 concept encourages a holistic approach to emergency communications by allowing public safety entities to build one core cybersecurity infrastructure that serves several agencies. This approach allows local authorities to share costs and benefit from comprehensive services and capabilities that might otherwise be cost-prohibitive. According to the FCC TFOPA final report:[26]

> *The TFOPA has determined that an additional layer should be introduced into the recommended future architecture. The intent of the logical architecture proposed in the form of the EC3 is to create a*

Figure 2: Emergency Communications Cybersecurity Center (EC3)



centralized function for securing NG networks and systems. By centralizing certain features, including cybersecurity in general and Intrusion Detection and Prevention Services (IDPS) specifically, public safety can take advantage of economies of scale, multiple resources, and systems and best practices that may already be in place or at a minimum readily available for deployment and use.

As illustrated in Figure 2, the potential flow of this system would begin with the originating service provider and NG9-1-1 core services elements, encompass the transport networks between ECCs, and provide for monitoring of call statistics, system health, anomaly detection, data sharing, mitigation, and recovery, while still allowing local agencies to maintain control of day-to-day operations.

To facilitate cybersecurity protections, the EC3 concept utilizes intrusion detection and prevention services (IDPS). This means the EC3 architecture has the capabilities to identify possible incidents, log information about them, attempt to stop them, and report them to security administrators.[27]

Inherent in the IDPS nature of the EC3 concept is the continuous monitoring of both voice and data networks to ensure a timely and efficient cybersecurity response. Several free resources assist ECCs in this effort through DHS CISA. Some of these free resources include:[28]

- Vulnerability scanning
- Web application scanning
- Phishing campaign assessment

In addition to outlining the EC3, the TFOPA reports also provide the following cybersecurity specific resources for ECCs to implement:

- Checklists to assist ECCs in assessing current cybersecurity posture.
- A roadmap of the cybersecurity lifecycle and assistance to achieve a more cyber secure posture.
- Cybersecurity use cases that are specific to emergency communications.
- Additional authoritative cybersecurity resources.

Developing a Response Plan to Cyberattack

Although ECCs can enhance cybersecurity awareness, it is essential that ECCs create a cyber incident response plan to guide employees in responding to an attack. In the instance that computers are unavailable, a printed copy should be provided to all staff. There are several resources that ECCs can rely on to create this document, including:

- National Institute of Science and Technology (NIST) Special Publication 800-61,[29] which outlines the four phases of an incident response lifecycle: preparation; detection and analysis; containment, eradication, and recovery, and post-incident activity (See Figure 3), and provides guidance on categorizing functional impacts, information impacts, and recoverability efforts.[30]
- The TFOPA reports, which include a generic template (complete with dependencies) to create a thoughtful approach to a cyber incident response plan based on the incident response lifecycle.[31]
- NIST Special Publication 800-61R2 that outlines 11 Crisis Handling Steps.[32]

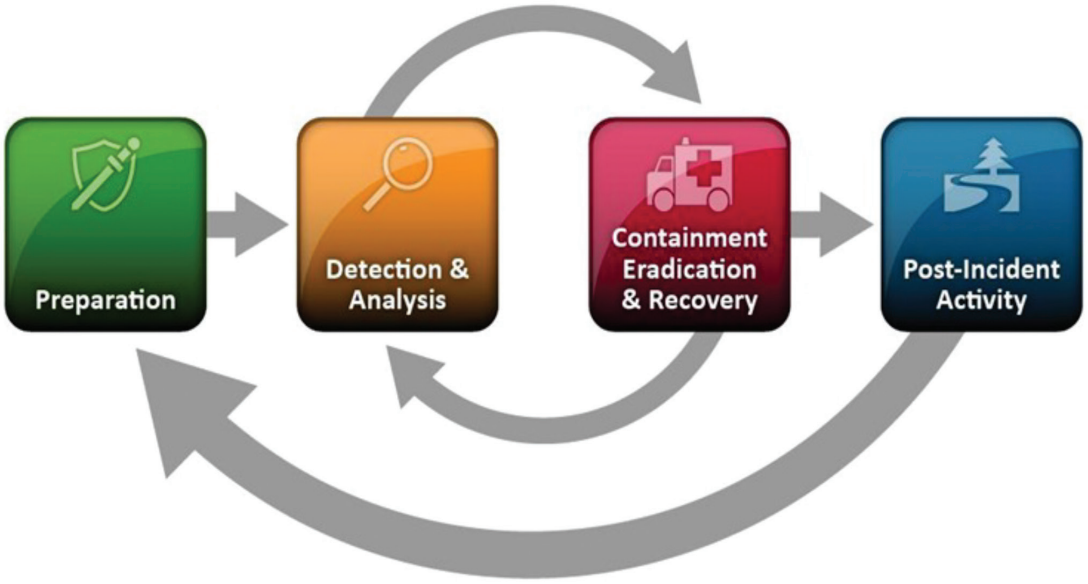
Cyber incident response plans may take several months to develop properly and should be created and maintained with the support of all jurisdictional stakeholders.

Once complete, ECCs should distribute the plan to all employees and conduct training to ensure that employees understand how to protect operations properly. Employees should maintain a printed copy of this plan in case networks are unavailable.

Improving Physical Security

For existing and future NG9-1-1 ECCs, strong cybersecurity practices should also include strong physical security practices. Developing a physical protection policy and procedures to safeguard hardware, software, media, and data from unauthorized access and use is essential. A systematic approach to physical security begins with performing an inventory of assets within the ECC, identifying potential vulnerabilities to the assets, identifying the potential threats,

Figure 3: Incident Response Lifecycle



understanding expected losses, and establishing a cyber incident response plan to prevent unauthorized access. Perimeter fencing, secured doors, locks, security cameras, and alarm systems assist in limiting access to secure areas of the ECC.

Secure and non-secured areas within the ECC should be prominently posted and separated by physical controls so that ECC personnel may verify individuals before allowing access. Risk is minimized when the ECC has an active list of authorized and credentialed personnel or deploy escorted access within the facility. Access should be limited to work areas minimally necessary to persons within the ECC, and devices that display PII or CJI must be positioned in a manner to prevent viewing by unauthorized persons.[33] Additionally, access to any physical components connected to the network and any unsecured workstation or external media control-removable hardware presents a significant risk of a cybersecurity attack, including when allowing bring your own device (BYOD) on the ECC system.

Cyber Training

The training of personnel to fully understand cybersecurity risks is a continual process that requires the fundamental recognition that networks, software, applications, and the devices and processes used within the ECC are significant targets for cyberattacks.[34]

A common phrase within cybersecurity circles is, "a system can be technologically the most secure system in the world, but there will always be a vulnerability – the people using the system." APCO has an ANSI-accredited standard titled "Cybersecurity Training for Public Safety Communications Personnel."[35] This standard recommends specific training for ECC personnel based on their role and the development of local policies and procedures, including on the topics addressed above. This standard recommends that designated ECC personnel devote at least four to eight hours annually to educating employees on policies and the employees' role in maintaining a security posture.

Developing and Implementing NG9-1-1 Policies and Procedures

Although the TFOPA report provides a framework for NG9-1-1 cybersecurity, ECCs must create policies and procedures to help guide employees toward a secure NG9-1-1 ecosystem. When creating these policies and procedures, it is essential to gather the perspective of jurisdictional stakeholders, including IT staff, ECC leadership, and any local

personnel that maintain systems and networks. Some examples of useful policies and procedures for cybersecurity include:

- Acceptable use policy
- Social media use
- Authentication procedures
- Password creation
- Email
- Remote access
- Endpoint protection

Chapter 7

KEY TAKEAWAYS

- The TFOPA report provides multiple resources specific to **enhancing cybersecurity for emergency communications**, including the EC3 concept, checklists for evaluating an ECC's cybersecurity posture, a roadmap of the cybersecurity lifecycle, and cybersecurity use cases.
- When implementing new hardware and software into the ECC, **local jurisdictions should work with vendors** to ensure that security updates will be provided.
- Jurisdictions should **create and maintain policies and procedures** to ensure an enhanced cybersecurity posture.
- ECCs are a high-value target for cybercriminals. **ECCs should create a cyber incident response plan** to guide employees through a response to a cyberattack.

23 *Project 43: Broadband Implications for the PSAP*, APCO International, at 37 (2017).

24 https://www.cisa.gov/known-exploited-vulnerabilities-catalog

25 Task Force on Optimal PSAP Architecture, Federal Communications Commission (2016) *available at* https://apps.fcc.gov/edocs_public/attachmatch/DA-16- 179A2.pdf.

26 transition.fcc.gov/pshs/911/TFOPA/TFOPA_FINALReport_012916.pdf

27 csrc.nist.gov/CSRC/media/Publications/sp/800-94/rev-1/draft/documents/draft_sp800-94-rev1.pdf

28 https://www.cisa.gov/cyber-hygiene-services

29 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

30 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

31 Task Force on Optimal PSAP Architecture, Federal Communications Commission (2016) *available at* https://apps.fcc.gov/edocs_public/attachmatch/DA-16- 179A2.pdf.

32 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

33 FBI, (2020). CJIS Security Policy (5.9). https://www.fbi.gov/file-repository/cjis_security_policy_v5-9_20200601.pdf

34 Bixler, M. & English, J. (2020). *Fundamentals of cybersecurity for the ECC*. APCO International: Alexandria, VA.

35 https://www.apcointl.org/~documents/standard/31101-2019-cybersecurity/?layout=default

Chapter 8
Legal Considerations

Historically, state and local governments establish laws regarding legacy 9-1-1 and some precursors to NG9-1-1 (e.g., ESInets). Federal agencies have more limited roles, such as setting requirements on service providers that originate 9-1-1 calls and carrying out federal grant programs. When it comes to NG9-1-1, federal regulations and congressional initiatives are emerging to shape national-level strategy and deployment while preserving state and local control. In some cases, legacy state laws hinder rather than facilitate the deployment of NG9-1-1. Effective laws at the federal, state, and local levels – and, relatedly, effective governance structures – would facilitate a more rapid and cost-effective transition to NG9-1-1. By adhering to key public safety principles such as interoperability and preserving state and local control, stakeholders at the federal and state level can pursue legal frameworks that best support NG9-1-1.

The Role of State and Local Laws and Regulations

The structure and provision of 9-1-1 service by ECCs is typically a state law matter, with some states further delegating aspects of 9-1-1 governance to the local level. Many states regulate the provision of legacy 9-1-1 service by incumbent local exchange carriers, usually under tariff regulations issued by the state public utility or public service commission.

A number of states have enacted laws and regulations to facilitate the deployment of precursors to NG9-1-1 (typically limited to call delivery via ESInet) by creating or improving governance structures, adopting deployment plans, creating and updating funding mechanisms, and promoting coordination, mutual aid, and information and resource sharing. Unfortunately, state laws and regulations may also hinder NG9-1-1 deployment. States may have outdated legislation and regulations that focus on legacy, circuit-switched technologies and processes, have outdated or insufficient funding and liability protection

Many states regulate the provision of legacy 9-1-1 service by incumbent local exchange carriers, usually under tariff regulations issued by the state public utility or public service commission.

schemes, or do not take a holistic approach to end-state NG9-1-1 deployment, all of which present obstacles to the deployment of NG9-1-1.

Federal Agencies With a Role Related to NG9-1-1

The FCC has broad regulatory authority over the provision of 9-1-1 service by commercial communications service providers. The FCC has adopted numerous regulations over the past two decades governing the provision of 9-1-1 and E9-1-1. These include regulations implementing 9-1-1 as the national emergency number and requiring all 9-1-1 calls to be routed to the appropriate ECC, E9-1-1 location accuracy requirements for wireless carriers, and E9-1-1 requirements for interconnected VoIP providers.

The National Telecommunications and Information Administration (NTIA) within the U.S. Department of Commerce and the National Highway Traffic Safety Administration (NHTSA) within the U.S. Department of Transportation are responsible for the joint 9-1-1 Implementation and Coordination Office (ICO). The ICO is required to: facilitate coordination and communications among public and private stakeholders at local, state, tribal, federal, and national levels; administer a grant program for the benefit of 9-1-1 centers across the country; and author or consult on several reports to Congress. As authorized by the Middle Class Tax Relief and Job Creation Act of 2012, NTIA and NHTSA awarded $109,250,000 of new funding for a

grant program to upgrade ECCs, including upgrades to NG9-1-1 capabilities. Prior to that, in 2009, NTIA and NHTSA administered an estimated $40 million grant program for 9-1-1 upgrades, authorized under the ENHANCE 9-1-1 Act.

Other federal agencies play important but generally less direct roles. For example, the Department of Homeland Security (DHS), through its SAFECOM program, works with state-level governance entities to improve multi-jurisdictional and intergovernmental communications interoperability. Historically within DHS, several FEMA grants that were not specifically designed for 9-1-1 could be used for 9-1-1 purposes and by extension NG9-1-1. Past programs with relevance for 9-1-1 stakeholders have included the Emergency Operations Center Grant Programs, Homeland Security Grant Program, Interoperable Emergency Communications Grant Program, Regional Catastrophic Preparedness Grant Program, and Tribal Homeland Security Grant Program.

Federal Laws Related to NG9-1-1[36]

While federal law does not govern NG9-1-1, there have been several federal laws related to 9-1-1. Here are examples of those laws that have implications for NG9-1-1.

- 1990 – Congress enacted the Americans with Disabilities Act (ADA), which, in part, prohibits state and local governmental programs from discriminating based on disability. The law was interpreted to require that local governments ensure that their telephone emergency number systems are equipped with technology that will give hearing impaired and speech impaired individuals a direct line to these emergency services. This mandate initially required the installation of TTY capabilities by ECCs, but Congress made clear that future technological advances may offer other means of affording direct and equally effective access for these individuals.[37]

- 1999 – Congress passed the Wireless Communications and Public Safety Act (9-1-1 Act).[38] The 9-1-1 Act required the FCC to designate 9-1-1 as the universal emergency telephone number within the United States for reporting an emergency to appropriate authorities and set the broad goal of facilitating "the prompt deployment throughout the United States of a seamless, ubiquitous, and reliable end-to-end infrastructure for communications, including wireless communications, to meet the Nation's public safety and other communications needs."[39] The 9-1-1 Act also grants wireless 9-1-1 service providers the same liability protection that a given state confers on its wireline carriers, and establishes that the ECC has the same immunity from liability regardless of whether the 9-1-1 call is made on a wireless or wireline system.[40] As described below, these protections were extended in the NET 9-1-1 Act and NG9-1-1 Advancement Act of 2012.

- 2004 – Congress enacted the Ensuring Needed Help Arrives Near Callers Employing 9-1-1 Act (ENHANCE 9-1-1 Act).[41] The act addressed numerous concerns that had been raised about 9-1-1 deployment, including compliance, coverage in rural areas, and the use of fees levied by states and localities to cover 9-1-1 service costs. The ENHANCE 9-1-1 Act also created the E9-1-1 Implementation and Coordination Office (ICO), an office jointly administered by NTIA and NHTSA, to assist and coordinate with state and local 9-1-1 authorities in the development of 9-1-1 and E9-1-1 and to administer a grant program for the implementation and operation of Phase II E9-1-1 services and NG9-1-1 services.[42]

- 2008 – Congress enacted the New and Emerging Technologies 9-1-1 Improvement Act (NET 9-1-1 Act).[43] The NET 9-1-1 Act confirmed the FCC's authority to regulate the provision of 9-1-1 by VoIP service providers and took other steps to improve the delivery of 9-1-1 services nationwide. Among other things, the Act also extended state liability protection for 9-1-1 and E9-1-1 to VoIP providers and other emergency service providers and required the FCC to report annually on collection of state fees and other levies on 9-1-1 and E9-1-1 services.

- 2010 – Congress enacted the Twenty-First Century Communications and Video Accessibility Act (CVAA).[44] The CVAA amended the Communications Act and imposed a variety of new obligations on service providers, equipment manufacturers, and the FCC that relate to providing access to communications services for people with disabilities. Under the CVAA, the FCC has authority to implement regulations, technical standards, protocols, and procedures that are necessary to achieve reliable, interoperable communication to ensure access by people with disabilities to an IP-enabled emergency network, where achievable and technically feasible.[45] As an example of how the CVAA relates to 9-1-1, the act was cited as one of the bases for the FCC's authority to adopt text-to-911 and real-time text rules.

The NET 9-1-1 Act confirmed the FCC's authority to regulate the provision of 9-1-1 by VoIP service providers and took other steps to improve the delivery of 9-1-1 services nationwide.

- 2012 – Congress enacted the Next Generation 9-1-1 Advancement Act of 2012 as part of the Middle-Class Tax Relief and Job Creation Act of 2012. This Act included several important provisions, including:
  - Reestablished the 9-1-1 ICO and established a matching grant program to support 9-1-1, E9-1-1, and NG9-1-1 implementation.
  - Defined "Next Generation 9-1-1 services" for the purpose of the reestablished ICO and established grant program.
  - Provided liability protection parity in the provision and use of NG9-1-1 services for NG9-1-1 service providers and users, ECCs, and associated officers, directors, employees, vendors, agents, and authorizing government entities. The act provides the same level of liability protection for NG9-1-1 that is afforded to wireless providers under the 9-1-1 Act, which is essentially the same level of liability protection that is afforded to

legacy 9-1-1 services under applicable state and federal law.

- Required ICO to submit a cost study to Congress, in consultation with NHTSA, the FCC, and DHS, that "analyzes and determines detailed costs for specific NG9-1-1 service requirements and specifications."
- Directed the FCC to prepare a report for Congress that contains recommendations for the legal and statutory framework for NG9-1-1.
- The report was delivered in 2013 and identified several recommendations for Congress to create a legal and regulatory environment that will assist states, ECCs, service providers and other stakeholders in accelerating the nationwide transition from legacy 9-1-1 to NG9-1-1. These recommendations included: create incentives for states to become early adopters of NG9-1-1; promote a consistent nationwide approach to key elements of NG9-1-1

deployment, including standards that support seamless communication among ECCs and between ECCs and emergency responders; reform the NG9-1-1 funding structure; and ensure appropriate liability protection to encourage technological innovation and rapid deployment of NG9-1-1.

Federal Regulations Related to NG9-1-1

While there are no federal regulations governing "NG9-1-1," the FCC has adopted numerous regulations governing the provision of 9-1-1 services. In 2001, the FCC's King County decision identified the demarcation point between wireless services providers and ECCs in the legacy E9-1-1 environment as the input to the 9-1-1 selective router.[46] The FCC has not identified a comparable demarcation point for allocating costs in an NG9-1-1 environment. However, the FCC has adopted rules that, taken together, can be viewed as assigning responsibility to originating service providers for routing IP-based multimedia communications to ECCs.[47]

The FCC has sought input related to regulatory issues with the implementation of NG9-1-1. Several issues have been raised: establishing authority over originating service providers' delivery of 9-1-1 services through ESInets; cost demarcation points in an NG9-1-1 environment; and preserving state/local authority over 9-1-1, among others.[48] As of writing, the FCC had not adopted rules to address NG9-1-1. However, some regulations might be considered as steps toward NG9-1-1 services.

OPPORTUNITIES TO SUPPORT NG9-1-1 BY UPDATING LAWS AND REGULATIONS

Avoid Shifting Responsibilities From Service Providers to Public Safety

When new regulations and laws are being debated, it is common for industry stakeholders to resist new obligations, often by shifting responsibility onto public safety agencies. This issue comes up in discussions of demarcation points and a variety of other contexts. Fundamentally, there is no reason to assume, particularly in an NG9-1-1 environment, that state or local 9-1-1 authorities need to take on responsibilities and costs that have been – or should be – with the service providers. Consider two examples of how this concept can be applied: location-based routing and interoperability testing.

Location-Based Routing

Historically, most wireless 9-1-1 calls have been routed through the cell site (tower) where the call is received and are sent to the ECC associated with that cell site. Sometimes, however, the 9-1-1 call is sent to the wrong ECC because the cell site where the call was received is not in the same jurisdiction as the 9-1-1 caller. Each time a wireless 9-1-1 call is routed to one ECC and must be transferred to another, the call transfer process consumes time and resources, and the process ultimately delays the ability of first responders to reach the scene of the emergency.

Location-based routing technologies allow carriers to route wireless 9-1-1 calls based on location information gathered from the handset, rather than the location of the cell tower. As handset-based location information has become more accurate

and more quickly available, location-based routing for 9-1-1 calls has become feasible. Some industry stakeholders have argued that location-based routing should be a feature of ESInet deployments and NG9-1-1 and left to 9-1-1 authorities to implement. Some industry stakeholders have even argued that wireless carriers are incapable of implementing location-based routing without support from 9-1-1 authorities. In June 2022, the FCC sought public input on how to route wireless 9-1-1 calls to the proper ECC more precisely.[49] The FCC incorporated several suggestions from APCO aiming to dispel misconceptions that location-based routing is dependent upon or equivalent to NG9-1-1, and to emphasize the fact that at least one nationwide carrier is providing location-based routing regardless of whether an ESInet or NG9-1-1 is in place. Thus, despite industry arguments to the contrary, a lifesaving enhancement such as location-based routing can be made for 9-1-1 without shifting responsibility from wireless service providers to ECCs.

Interoperability Testing

In the context of NG9-1-1 and the definitions developed by the public safety community, interoperability must be achieved without the use of proprietary interfaces. To do this, service providers and vendors can leverage industry standards to deliver solutions that are interoperable for ECCs without customizations, proprietary interfaces, or after-the-fact expenses. The telecommunications industry offers interoperable solutions for IP-based services; consumers can choose devices and service providers without concern that these choices will limit the interoperability of their communications. Vendors achieve interoperability through methods such as conformance testing and end-to-end interoperability testing. Consider for example a particular brand and model of a smartphone. By the time it is offered for sale, the industry has already taken the steps necessary to ensure that the consumer receives a product that simply works with other smartphones, networks, apps, etc. The vendor ensured that the smartphone conforms to the standards used in the communications industry for interoperability and other features. The vendor would also have typically conducted testing to make sure that the smartphone can interoperate from receipt of a message, through the various connecting networks, and to a receiving device.

The industry should be responsible for delivering interoperable solutions and developing and funding whatever processes are needed to do so.

In contrast, some stakeholders have suggested that interoperability be achieved for NG9-1-1 services by establishing a testing and certification process that would be overseen and funded by the public safety community and/or the federal government. This would inappropriately shift responsibility from the service providers, introduce inefficiencies, and likely increase costs for public safety agencies. The industry should be responsible for delivering interoperable solutions and developing and funding whatever processes are needed to do so. Ensuring that the industry bears responsibility for achieving interoperability will be easier if ECCs adhere to a common vision for NG9-1-1, which would be facilitated by a significant federal NG9-1-1 grant program that requires interoperability, and/or through RFPs that specify interoperability as a requirement.

---

36 While not discussed in detail here, there are two federal laws pertaining to privacy and confidentiality that may be of general interest. First, the Health Insurance Portability and Accountability Act (HIPAA) is a comprehensive federal healthcare privacy law that regulates the disclosure of protected healthcare information by certain covered entities. ECCs, however, are not beholden to these requirements because they are not considered a covered entity. Additionally, HIPAA includes certain exemptions for use of the information by public safety or law enforcement. See 45 C.F.R. § 160.103.

Second, service providers maintain a duty to provide confidentiality protections to their customers. Under the Communications Act, service providers are prohibited from disclosing personally identifiable customer information without permission, yet an exception exists for disclosing the location information of a caller to an ECC. See 47 CFR § 222(d)(4).

37 H.R. Rep. No. 101-485, pt. 2, at 84-5 (1990). Similar language is found in the ADA Conference Committee Report. H.R. Rep. No. 101-596, at 67-8 (1990) (Conf. Rep.).

Chapter 8

KEY TAKEAWAYS

- No federal laws or regulations govern "NG9-1-1," but **several existing laws and regulations have implications for and will likely extend into** an NG9-1-1 environment.
- **States should address outdated laws and regulations** that will inhibit the transition to NG9-1-1.
- All levels of **government should avoid legislative, regulatory, and procurement approaches that shift responsibility from service providers** to public safety agencies.
- Federal support is needed for the nationwide transition to NG9-1-1, but **we should preserve state and local control of 9-1-1**.

[38] Wireless Communications and Public Safety Act, Pub. L. No. 106-81, § 3(a), 113 Stat. 1286 (1999) (codified at 47 U.S.C. §§ 222, 251, 601, 615, 615a, and 615b) ("9-1-1 Act").

[39] *Id.* § 2 (codified at 47 U.S.C. § 615 note (b) (1999).

[40] *Id.* § 4 (codified at 47 U.S.C. § 615a).

[41] Ensuring Needed Help Arrives Near Callers Employing (ENHANCE) 9-1-1 Act, Pub. L. 108-498, §§ 104, 158(b)(1), 118 Stat. 3987-3988 (2004) (codified as amended at 47 U.S.C. §§ 901, 942 (2008)) ("ENHANCE 9-1-1 Act").

[42] *Id.* § 104 (codified as amended at 47 U.S.C. § 942 (2008)).

[43] New and Emerging Technologies 9-1-1 Improvement Act, Pub. L. 110-283, 122 Stat. 2620 (2008) (codified at 47 U.S.C. §§ 222, 609, 615a-b, 942) ("NET 9-1-1 Act").

[44] Twenty-First Century Communications and Video Accessibility Act, Pub. L. No. 111-260, 124 Stat. 2751 (2010) (as codified in 47 U.S.C. §§ 64.6201, 64.6203, 64.6205, 64.6207, 64.6209, 64.6211, 64.6213, 64.6215, 64.6217, 64.6219) ("CVAA").

[45] *Id.* § 106(g) (codified at 47 U.S.C. § 615c(g)) (providing that "[t]he Commission shall have the authority to promulgate regulations to implement the recommendations proposed by the [Emergency Access Advisory Committee], as well as any other regulations, technical standards, protocols, and procedures as are necessary to achieve reliable, interoperable communication that ensures access by individuals with disabilities to an Internet protocol-enabled emergency network, where achievable and technically feasible.").

[46] *See* Letter from Thomas J. Sugrue, Chief, Wireless Telecommunications Bureau, to Marlys R. Davis, E911 Program Manager, Department of Information and Administrative Services, King County, Washington, CC Docket No. 94-102, at 3 (filed May 7, 2001); *See also* Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems, Request of King County, Washington, CC Docket No. 94-102, *Order on Reconsideration*, 17 FCC Rcd 14789, at para. 3 (2002).

[47] *See* Comments of APCO International, Public Safety and Homeland Security Bureau Seeks Comment on Petition for Rulemaking Filed by the National Association of State 9-1-1 Administrators, PS Docket No. 21-479, *Public Notice*, DA 21-1607 (filed Jan. 19, 2022) (describing text-to-9-1-1 and RTT requirements) *available at* https://www.apcointl.org/~documents/filing/apco-comments-nasna-ng911-petition-011922?layout=default.

[48] *See* Public Safety and Homeland Security Bureau Seeks Comment on Petition for Rulemaking Filed by the National Association of State 9-1-1 Administrators, PS Docket No. 21-479, *Public Notice*, DA 21-1607 (rel. Dec. 20, 2021) *available at* https://www.fcc.gov/document/pshsb-seeks-comment-nasna-petition-rulemaking.

[49] Federal Communications Commission Seeks to Refresh the Record on Location-Based Routing for Wireless 911 Calls, PS Docket 18-64, *Public Notice*, FCC 22-42 (2022) *available at* https://www.fcc.gov/document/fcc-examines-location-based-routing-wireless-911-calls-0.

Chapter 9

Conclusions and Next Steps

Modern technologies in use today, and those yet to be developed, will allow ECCs to play an increasingly impactful role in emergency response. The promise of NG9-1-1 can only be achieved, however, if the 9-1-1 community works toward a shared vision that aligns with core public safety principles like interoperability, security, and innovation.

NG9-1-1 has the potential to meet public expectations by matching the capabilities the public uses to communicate daily. Sharing texts, photos, videos, and all types of data including location information directly with the ECC allows PSTs to receive any type of request for emergency assistance regardless of the type of device and service provider. The most critical part of call management begins with the PST receiving a message reporting the emergency without delay.

The following strategies summarize key recommendations presented in this guide.

1. Upgrade Your Procurements

9-1-1 authorities and ECCs should make their requirements clear to vendors. As discussed in Chapter 4 and Chapter 5, this can include rethinking how to craft RFPs by stating public safety objectives – such as full interoperability, reliability, security, and end-to-end solutions.

2. Do Not Assume Responsibilities That Belong to Vendors

New capabilities for 9-1-1, particularly those associated with regulatory or legislative proceedings, often present a debate over how to allocate costs and responsibilities between the industry and public safety agencies. At every opportunity, the public safety community should press for taking advantage of the industry's superior economies of scale. For example, to achieve interoperability, there is no reason the vendor community should not resolve the impediments under its control, conduct all necessary testing, and then offer solutions that meet public safety's needs.

3. Seek Full Solutions

NG9-1-1 must be fully interoperable, secure, and capable of receiving and sharing any request for emergency assistance without customized and propriety solutions.

Limited deployments of precursor technologies, i.e., ESInets and related functional elements, are only one part of NG9-1-1 and will in the long term extend the transition time, cost more, and prolong the status quo of proprietary, non-interoperable systems.

At every opportunity, the public safety community should press for taking advantage of the industry's superior economies of scale.

4. Take Advantage of Modern Technology

ESInets do not provide a complete NG9-1-1 solution (leaving out altogether the dispatch/CAD portion) and place the responsibility on 9-1-1 authorities to implement the IP connectivity needed at the call handling side as well as the related functional elements. Further, ESInet deployments are plagued by lack of interoperability, limited functionality (i.e., support IP-based voice only), stranded investments, and equipment obsolescence. These problems are partially rooted in the early conceptualizations of NG9-1-1 that have not evolved with developments in the broader communications industry.

Today many technologies exist that produce significant economies of scale while meeting public safety needs and keeping responsibility for provision of NG9-1-1 services with the vendors versus shifting to public safety. ECCs can change the current course and obtain holistic solutions that meet all their needs and avoid shifting responsibilities to public safety.

5. Support Efforts for Major Federal Funding

The nation's major public safety associations are pressing Congress to enact a significant federal funding program to implement NG9-1-1 nationwide along with key public safety requirements as conditions of grant funding, including interoperability, reliability, and cybersecurity. With the right conditions, the prospect of significant federal funding, and congressional oversight, the vendor community will be much more likely to deliver the NG9-1-1 solutions that public safety needs.

ECCs can change the current course and obtain holistic solutions that meet all their needs and avoid shifting responsibilities to public safety.

Appendix

APCO Sample RFP Template for NG9-1-1 Capabilities

Preface

APCO has prepared this Sample RFP Template for NG9-1-1 Capabilities to assist 9-1-1 directors and authorities with their procurement activities. This document is intended to address several concerns APCO has identified with the state of progress toward NG9-1-1. Additionally, the document is intended to be used as a ***guide*** for agencies, not as a "cut and paste" document.

While the APCO RFP Template is comprehensive in nature and designed to cover all aspects of a complete NG9-1-1 deployment, regardless of the stage any state or locality is in concerning the transition to NG9-1-1, it does not include agency specific information. This is by design in order to allow the agency to incorporate any information specific to their existing solution and/or future needs.

The Template offers recommendations, guidance, and suggested specific operational requirements that will be of interest to any state or local official involved in the procurement process. This applies to both State and Local 9-1-1 officials and directors and managers of emergency communications centers (ECCs).

This template is not specifically designed for any level of system. In other words, the intent is to allow agencies of all levels to use any part of the document they consider relevant and helpful. The document is also not intended to specify any specific level of network (Statewide vs Regional vs Local), instead the intent is to provide enough information for officials at any level of government to utilize any or all of the document they find useful.

Introduction

This section of the RFP should contain an overall description of the project, Executive Summary and potentially contract requirements at high level only. This is the agency's opportunity to outline exactly what operational capabilities are expected of the system. Some sample language is included below for use by the agency as they see fit.

Project Description

The agency should define its specific system, and requirements, in this section. The language below is meant only as a guide for the agency to work with.

Our agency is seeking a qualified and experienced contractor or contractors to provide a Next Generation 9-1-1 (NG9-1-1) system to process all calls placed to 9-1-1 regardless of the network of origin (PSTN, VoIP, or other IP based originating sources) or type of call (IP, Analog, Text, Multimedia Data, etc.).

The agency recognizes that a robust NG9-1-1 system capable of processing all Requests for Emergency Assistance (RFEA)[50] in an efficient and accurate manner is critical to the safety of both the public and field responders. The agency desires to purchase an NG9-1-1 system that will meet both its current and future needs. Reduced overall system cost is certainly a goal. However, interoperability, innovation, cybersecurity, enhanced capability, remote diagnostics, and a system architecture designed to accept future types of calls are some of the most important objectives of this project.

The intent of this RFP is to replace the existing system(s) with a true NG9-1-1 solution. This RFP focuses on supporting a complete turnkey installation that meets all operational requirements and includes specifications for not only interconnected systems but truly interoperable systems.

The importance of interoperability cannot be over-stressed. The agency incorporates the following definition of interoperability.

"…the capability of emergency communications centers[51] to receive 9-1-1 requests for emergency assistance and related data such as location information and callback numbers from the public, then process and share the 9-1-1 requests for emergency assistance and related data with other emergency communications centers and emergency response providers,[52] regardless of jurisdiction, equipment, device, software, service provider, or other relevant factors, and without the need for proprietary interfaces."

The agency seeks a comprehensive NG9-1-1 solution as an interoperable, secure, IP-based system that—

- Enables the appropriate ECC to receive, process, and analyze all types of 9-1-1 Requests for Emergency Assistance;
- Acquires and integrates additional information useful to handling NG9-1-1 Requests for Emergency Assistance; and
- Supports sharing information related to 9-1-1 Requests for Emergency Assistance among ECCs and emergency response providers.

This document provides the minimum requirements for the system along with options and required NG9-1-1 network interfaces. The intent of this document is to provide the requirements for a fully enabled NG9-1-1 solution. It is not the intent to provide details that would focus the vendor's solutions toward a specific technology or standard.

Vendors shall provide their individual solution(s) and products configured in a manner consistent with the definition of NG9-1-1. Furthermore, interoperability is a requirement from the onset.

It is the vendor's responsibility to identify any additional partnerships that may be required to facilitate compliance with this requirement, and any additional costs must be clearly identified in this response. The vendor shall provide specific information as to how it will achieve interoperability, what specific elements the solution will contain, and all partnerships that will be included. Failure to comply with these requirements may result in automatic disqualification of the vendor.

Agencies can then expand on any specific objectives, operational needs/requirements, and unique local aspects of this RFP.

As noted above, this RFP does not define a particular solution. The agency seeks to achieve the following primary objectives:

1. Cost-effectiveness
2. Interoperability
3. Multimedia capability
4. Compatibility with current and emerging consumer and responder broadband technologies
5. Cybersecurity

Vendors shall describe how they will achieve these objectives through delivering a solution utilizing the required operational requirements identified herein.

Pre-Bid Conference

(*Placeholder for agency specific dates/information*)

Calendar of Events

(*Placeholder for agency specific dates/information*)

General Instructions

(*Placeholder for agency specific dates/information*)

Should include:

1. Cost of Developing RFP
2. RFP Ownership
3. Preparing and Submitting a Proposal
4. Vendor Qualifications
   a. This section should include specifics as to what types of references the agency expects. Vendor responses should:
      i. Include all clients who have awarded contract to vendor in the last ten years;
      ii. Note specifically which solution, system, and version number was supplied to these clients; and
      iii. Supply a list of clients that the vendor has lost over the last five years (which is not necessarily an indication of dissatisfied clients as this may be due to budgetary or other considerations).

General Instructions

The evaluation and selection of a contractor and the contract will be based on the information submitted in the vendor's proposal plus references and any required on-site visits or oral presentations.

Each point by point response from the bidder must be answered with one of the following responses:

Comply – The proposed solution will fully meet the requirement(s), functionality is currently supported in the current product software release.

Exception – The proposed solution complies partially with this requirement; with exceptions explained in detail. If a vendor takes exception but an alternative to the requirement is recommended, the alternative must be explained, and any cost identified. Exceptions will be evaluated and considered but are not necessarily acceptable solutions to the requirement as expressed nor are they automatic disqualifications.

Does Not Comply – The proposed solution does not fully comply with this requirement.

Vendor Response / Explanation –
All responses require a detailed explanation of the vendor's answer.

Respondents must complete and return the entire RFP packet. Once all packets have been received, opened, and recorded, a team representing system users and the agency will evaluate the information provided and make a recommendation to the purchasing authority. The agency shall be the sole judge in determining how

the evaluation process shall be conducted and what vendors shall be considered.

The Agency may conduct such investigations, as it considers necessary, to assist in the evaluation of vendor-provided information to establish the responsibility, qualifications, and financial ability of any potential vendor.

Vendors are expected to put forth their "best and final" pricing as a component of this bid. While price will not be the only factor considered in selecting a vendor, cost to the organization is a critical factor.

The Agency reserves the right to reject any and all proposals, in part or in whole, and to award to the most responsive and responsible firms as deemed in the best interests of the agency; further, the right is reserved to waive any formalities or informalities contained in said proposals.

All proposals and copies thereof are to be prepared and submitted at the submitter's expense. Also note, upon submittal to the Agency, the proposals may become public record and are subject to the Agency's FOIA guidelines. The respondent may request certain sections of the response that contain proprietary business intelligence or system technical details be redacted if such redaction is allowed under agency policy and governing law.

Background on Current Environment (Need/Problem)

A new NG9-1-1 system is necessary because …… (*Placeholder for agency specific information*)

Service Level Agreements (SLAs)

This section will delve into service level agreement requirements that any potential vendor will be held to. This section becomes particularly important in enforcing operational capabilities and should include specific attention to what the vendors are required to deliver upon initial implementation and what would also be required to satisfy the ongoing, and evolving, capabilities of a true NG9-1-1 center. If your agency proceeds in stages toward a full NG9-1-1 solution (such as by proceeding with an ESInet alone, or a call handling or CAD-only solution), the vendors should be put on notice that you intend to eventually achieve a complete NG9-1-1 solution, which should not entail any specialized or proprietary technologies that would hinder complete interoperability or lead to excessive costs. In short, this is the opportunity for the agency to specify that it expects vendors to describe how their solutions would facilitate future integrations with remaining components of a fully interoperable NG9-1-1 system, including if, why, and how their particular solution would add any costs or complexities that would ordinarily not be expected with other widely deployed consumer and responder broadband communications solutions.

A service-level agreement (SLA) defines the level of service expected by a customer from a supplier, laying out the metrics by which that service is measured, and the remedies or penalties, if any, should the agreed-on service levels not be achieved. For the purpose of this RFP the SLAs are between the agency and all external suppliers. SLAs are a critical component of any technology vendor contract. Beyond listing expectations of service type and quality, an SLA provides remedies when requirements aren't met.

As addressed elsewhere in this RFP, network availability of 99.999 percent is expected. Documentation (proof) of this claim is required.

The SLA should include components in two areas: services and management.

Service elements include specifics of services provided (and what's excluded, if there's room for doubt), conditions of service availability, standards such as time window for each level of service (prime time and non-prime time may have different service levels, for example), responsibilities of each party, escalation procedures, and cost/service tradeoffs.

Management elements should include definitions of measurement standards and methods, reporting processes, contents and frequency, a dispute resolution process, an indemnification clause protecting the customer from third-party litigation resulting from service level breaches (this should already be covered in the contract, however), and a mechanism for updating the agreement as required. This last item is critical; service requirements and

vendor capabilities change, so there must be a way to make sure the SLA is kept up to date.

An **indemnification clause** is an important provision in which the service provider agrees to indemnify the customer company for any breaches of its warranties. Indemnification means that the provider will have to pay the customer for any third-party litigation costs resulting from its breach of the warranties. *If you use a standard SLA provided by the service provider, it is likely this provision will be absent; ask your in-house counsel to draft a simple provision to include it, although the service provider may want further negotiation of this point.*

Most service providers make **statistics** available, often via an online portal. There, customers can check whether SLAs are being met, and whether they're entitled to service credits or other penalties as laid out in the SLA.

The following metrics, responsibilities and expectations are minimum requirements:

Service availability: the amount of time the service is available for use. This may be measured by time slot, with, for example, 99.5 percent availability required between the hours of 8 a.m. and 6 p.m., and more or less availability specified during other times. E-commerce operations typically have extremely aggressive SLAs at all times; 99.999 percent uptime is not an uncommon requirement for a site that generates millions of dollars an hour.

Defect rates: Counts or percentages of errors in major deliverables. Production failures such as incomplete backups and restores, coding errors/rework, and missed deadlines may be included in this category.

Technical quality: In outsourced application development, measurement of technical quality by commercial analysis tools that examine factors such as program size and coding defects.

Security: Application and network security breaches can be costly. Measuring controllable security measures such as anti-virus updates and patching is key in proving all reasonable preventive measures were taken, in the event of an incident.

Business results: Increasingly, IT customers would like to incorporate business process metrics into their SLAs. Using existing *key performance indicators* (KPIs) is typically the best approach as long as the vendor's contribution to those KPIs can be calculated.

In the event of issues with the service, neither party can plead ignorance. It ensures both sides have the same understanding of requirements. In addition, the SLA should be reviewed by legal counsel to ensure it is not open to deliberate or inadvertent misinterpretation. Misalignment can have a negative impact on deal pricing, quality of service delivery, and customer experience.

Most service providers have standard SLAs – sometimes several, reflecting various levels of service at different prices – that can be a good starting point for negotiation. However, since they are usually slanted in favor of the supplier these should be reviewed and modified by the customer and legal counsel.

The SLA should include not only a description of the services to be provided and their expected service levels, but also metrics by which the services are measured, the duties and responsibilities of each party, the remedies or penalties for breach, and a protocol for adding and removing metrics.

Metrics should be designed so bad behavior by either party is not rewarded. For example, if a service level is breached because the client did not provide information in a timely manner, the supplier should not be penalized.

For critical services, agencies may want to consider investing in third-party tools to automatically capture SLA performance data, which provide an objective measure of performance.

The types of SLA metrics required will depend on the services being provided. Many items can be monitored as part of an SLA, but the scheme should be kept as simple as possible to avoid confusion and excessive cost on either side. In choosing metrics, examine your operation and decide what is most important. The more complex the monitoring (and associated remedy) scheme, the less likely it is to be effective, since no one will have time to properly

analyze the data. When in doubt, opt for ease of collection of metric data; automated systems are best, since it is unlikely that costly manual collection of metrics will be reliable.

The goal should be an equitable incorporation of best practices and requirements that will maintain service performance and avoid additional costs. The first goal of any metric is to motivate the appropriate behavior on behalf of the client and the service provider. Each side of the relationship will attempt to optimize its actions to meet the performance objectives defined by the metrics. First, focus on the behavior that you want to motivate. Then, test your metrics by putting yourself in the place of the other side. How would you optimize your performance? Does that optimization support the originally desired results?

Less is more. Despite the temptation to control as many factors as possible, avoid choosing an excessive number of metrics or metrics that produce a voluminous amount of data that no one will have time to analyze and create excessive overhead. While less likely, too few metrics are also a problem as missing any one may mean the provider has breached the contract.

Set a proper baseline. Defining the right metrics is only half of the battle. To be useful, the metrics must be set to reasonable, attainable performance levels. Unless strong historical measurement data is available, be prepared to revisit and readjust the settings at a future date through a predefined process specified in the SLA.

Define with care. A provider may tweak SLA definitions to ensure they are met. For example, the Incident Response Time metric is supposed to ensure that the provider addresses an incident within a maximum number of minutes. However, some providers may meet the SLA 100 percent of the time by delivering an automated reply to an incident report. Customers should define SLAs clearly so that they represent the intention of the service level.

In addition to defining the services to be provided, the contract should also document how the services are to be monitored, including how the data will be captured and reported, how often it will be reviewed, and who is involved in the review.

System and Training Documentation

The vendor is expected to provide detailed system and training documentation to the agency. This response should include specific type, name, and number of documents that are to be provided to the agency. Please note that a single copy of any document is not sufficient. Vendor should plan and respond accordingly.

Suggested Minimum Documentation

As-builts

Two complete sets of as-built drawings are required. As-built drawings must be submitted in a Microsoft Visio format, or other agreed upon graphic format as delineated in the contract, on two individual sets of CDs. The installation and acceptance of the system shall not be complete until as-built drawings are delivered.

Manuals

Provide documentation for installation, operation, and maintenance for each component of the system. This documentation will include user manuals, maintenance manuals, and parts list of the equipment necessary for the continued and proper preventative maintenance and repair.

Training Requirements

Training on all system functions must be provided by the vendor prior to acceptance of the system. Training must include sufficient information and experience to familiarize personnel (administration and supervisors) with all system functions, features, and operations for their particular assignments.

The vendor must implement a train-the-trainer plan for telecommunicators and ECC administrators. Describe how you will meet this requirement.

Training Curriculum

The vendor shall include in its proposal a training curriculum for telecommunicators, administrators, and County training instructors. The training curriculum shall include instruction on all aspects

of the ECC/Intelligent Workstations, including but not limited to the following:

a) Call taking
b) System Administration & Customization
c) Reporting

Training Material

Training materials for telecommunicators, administrators, and training instructors shall be approved by the agency prior to the delivery of any training. Training materials shall become the property of Combined Dispatch.

Participants must receive individual copies of applicable training materials at the time the course is conducted. Authorization shall be granted to reproduce these and any subsequent training materials that are provided. It is a requirement that sufficient copies of ANI/ALI Controller end user training documentation and copies of administrative training documentation be included in this project in CD or DVD format in addition to paper for each participant.

Training Schedule

Training schedule shall be approved by the agency.

Project Management

Project Manager

It is required that the vendor assign project managers who are familiar with 9-1-1 networks and IP networks, as well as the proposed system. It is a requirement that the proposal include the project manager's resume with references and experiences on similar projects.

Project Plan

The vendor is required to submit a task-oriented Gantt chart detailing the system installation utilizing the most recent version of MS Project (or agreed upon equivalent). The proposed start date for the project must utilize a "contract date" for competitive and demonstrative purposes. The project plan must identify critical dependencies and typical timelines.

---

50 The term "9-1-1 request for emergency assistance" means a communication, such as voice, text, picture, multimedia, or any other type of data that is sent to an emergency communications center for the purpose of requesting emergency assistance

51 The term "emergency communications center" means a facility that is designated to receive a 9-1-1 request for emergency assistance and perform one or more of the following functions:
A. Process and analyze 9–1–1 requests for emergency assistance and other gathered information.
B. Dispatch appropriate emergency response providers.
C. Transfer or exchange 9–1–1 requests for emergency assistance and other gathered information with other emergency communications centers and emergency response providers.
D. Analyze any communications received from emergency response providers.
E. Support incident command functions.

52 The term "emergency response provider" includes federal, state, and local governmental and nongovernmental emergency public safety, fire, law enforcement, emergency response, emergency medical (including hospital emergency facilities), and related personnel, agencies, and authorities.

Statement of Work (SOW) and Technical Details (NG9-1-1)

This section of the RFP will be used by the agency to define the statement of work, including operational requirements, and specific technical requirements for the NG9-1-1 call/Request for Emergency Assistance (RFEA) handling portion of the overall solution. There are two distinct functional sections of this RFP. This first section will address initial call handling and processing of RFEAs. The second major section will address computer aided dispatch (CAD), records management system (RMS), and mobile data. Certain aspects of incident handling that are more specific to the call processing components, such as recording, logging, and reporting specific to call receipt, will be handled in this section as well.

Technical Requirements / NG Functionality

This RFP focuses on meeting actual, operational needs of the ECC. The operational functions include interoperable, multimedia capable systems. In addition, the system shall not require a forklift upgrade to deliver NG9-1-1 functionality at any point along the migration path to true NG9-1-1. The agency intends to participate as part of an ESInet or equivalent commercially available, secure transport system. The agency requires that any solution be completely integrated with, and interoperable with, the selected ESInet or network transport solution. This means that the agency's ESInet shall be interoperable with other ESInets regardless of vendor or jurisdiction. Any prospective vendor must show the solution is scalable and adaptable based on emerging public safety needs. The agency will give preference to any solution that meets operational needs, and provides the same, or better, levels of innovative, interoperable, multimedia capable services that are already widely available to the public.

Rather than a dogmatic approach, referring only to certain standards that traditionally allow for proprietary implementations, inhibit (or preclude) interoperability, and/or result in additional costs for frequent upgrades, this RFP specifies functional requirements to meet actual operational needs of the agency. Instead of relying on prevailing architectures and functional elements, this document seeks vendors who can provide innovative, functional equivalents based on open architectures that facilitate interoperable, secure, multimedia-based communications.

NG9-1-1 Core Network

Core services provide call routing intelligence in an NG9-1-1 system. These services ensure that traffic initiated on, destined for, and processed by ECCs remains discrete from public traffic, secure, and properly routed. While some documents and standards define specific elements that are required, the intent of this RFP is to deliver a solution that meets the functional needs of the ECC. Responses that simply declare compliance with any particular standard are not sufficient, as they often lead to proprietary, non-interoperable, and excessively costly results. There are a number of ways to ensure proper call routing, verification, security, location data, and multimedia capabilities. While some documents, such as the NENA i3 document or ATIS IMS to ESInet, include partial functionality for each of these areas, no single standard currently enables a fully functional, interoperable, multimedia capable solution. According to the National 9-1-1 Program Office, "Using NENA's i3 standard alone is not the same as an NG9-1-1 system."[53]

As a result, this RFP requires potential vendors to describe how they achieve functions, not merely adhere to certain documents and standards, and to

verify the interoperable, multimedia capable nature of the proposed solution.

❑ **Comply**
❑ **Exception**
❑ **Does Not Comply**
Vendor Response / Explanation: _____

PST Workstation and Workflow

What follows are suggested minimum requirements for Telecommunicator workstations. This is not meant to be an exhaustive list, nor is it meant to preclude any agency from including additional requirements or removing any of those suggested below. These are simply suggested functions for the agency to consider including.

The workstation should be state-of-the-art, digital technology, with the most modern processor and computing capabilities available in the market at the time of implementation. If included in the bid, the workstation must be equipped with all necessary audio and video interface equipment to include keyboard, mouse, speakers, and flat panel monitor (size and additional specifications at discretion of the agency).

Headset/Handset

The workstation shall provide an analog audio interface to a headset/handset and to the radio system / dispatch unit to accommodate both radio and 9-1-1 audio in the same headset/handset.

Radio Integration

The workstation must be interfaced/integrated with the radio system. Telecommunicators shall use the same headset for both radio and telephone conversations.

9-1-1 Client Software Requirements

The 9-1-1 client software must be compatible with Microsoft Windows™ latest operating system. Windows 7 is NOT an option. The screen layout must be customizable. If a fault occurs in the application or on a PC while a call is active the call must be presented to another Telecommunicator.

Telecommunicator Log-on

The system shall require Users to log-on with a Username/Password combination. Upon successful completion of the log-on, each Telecommunicator will be presented with a selection of pre-configured roles.

The screen layout presented to the Telecommunicator shall be based on a user/role combination. If a user/role combination has not been defined for the Telecommunicator then the screen layout presented to the Telecommunicator shall be based solely on the selected role. If a role has not been assigned to the Telecommunicator, the Default User/Default Role layout shall be presented. Telecommunicators shall be able to log-on at any position and be presented with the identical screen layout associated with the selected role.

Call / Line Indicators

The workstation shall indicate incoming emergency and non-emergency calls by both audible and visual means. 9-1-1 trunks shall have a different audible and visual signal from other lines. The workstation shall have the ability to visually display the status (connected, ringing, or on hold) of each emergency and non-emergency call.

Routing Status

It is desirable that the workstation be capable of providing a visual display of the routing status of the call:

Normal – the first attempt to route the call was successful

Overflow – the first route was busy or congested

Alternate – the first route attempt failed, and another route was attempted

Transfer – the call was transferred

Not Available – no routing status was received.

Graphical User Interface

The GUI must consist of a number of windows, each of which can be located and docked in a position on the screen deemed most optimal by the agency.

Screen Layout Lock

The screen layout shall be automatically locked when the Telecommunicator logs in to the answering position.

Print Capabilities

The workstation shall provide an interface port for manual printing of ALI and TDD conversation upon call release. It is required that the workstation is able to send print jobs to a network printer.

Status Windows

The workstation shall present the telecommunicator with the status of the following categories:

- Number of Active 9-1-1 Calls
- Number of 9-1-1 Calls on Hold
- Number of 9-1-1 Calls Ringing
- Number of Active Call Takers

The numbers shall be summarized and presented on icons. Telecommunicators shall be able to open up windows for each status category to obtain more information about calls in each category to include:

- ANI
- Trunk
- Position
- Call Taker
- Start Time

Automatic Number Identification

The workstation must be capable of providing visual display of the emergency caller's telephone number.

Automatic Location Identification

The workstation shall be capable of providing visual display of the calling party's street address information based on the information received from either legacy ANI or IP-based calling party number information. The workstation must also be capable of extracting geographical coordinate information from the ALI file, or IP equivalent data, received and transmitting this information to geographical mapping software.

Wireless Call Handling

The workstation shall present wireless calls and shall include all standard call handling features.

Single step wireless callback is mandatory as the Telecommunicator shall not be required to perform a manual ANI callback for wireless calls.

TDD Detection

The workstation shall be capable of detecting emergency calls originating from Baudot- type Telecommunication Devices for the Deaf (TDD) equipment and indicating to the telecommunicator the presence of the TDD call.

TDD Communication

The workstation must allow telecommunicators to communicate with TDD/TTY callers directly from their 9-1-1 workstation keyboard, without requiring the use of any external device.

Telecommunicators must also be capable of manually connecting to emergency calls originating from ASCII-type TDD/TTY equipment, as well as originating both Baudot and ASCII calls from their answering position.

RTT Communication

The workstation, and overall system, must support Real-Time Text (RTT) when the technology is made available to ECCs and should do so without additional cost to the ECC.

Call Review

The workstation shall allow the telecommunicator to view the ANI information of at least the last 10 calls released at the answering position.

Instant Messaging

Instant messaging must be available from each agency workstation and be configurable or disabled according to individual agency requirements. Each workstation shall have the ability to send an instant message to any other workstation on the system.

Automatic ALI Rebid

The workstation shall automatically update X/Y coordinates at regular intervals. This feature shall be configurable as to the number and frequency of intervals on a per wireless provider basis or as a universal system setting.

ALI Parsing

The workstation shall guarantee that ALI data is appropriately and consistently displayed when interfacing with different ALI providers that send their information in various formats (i.e. wireline vs. wireless).

Conference

The workstation must provide the telecommunicator the ability to remain on a call and add a new party to the conversation without putting the caller on hold – the caller must remain on-line at all times.

The system shall allow for up to 10 simultaneous conferences of up to 10 parties each.

Any party shall be able to drop out of the conference, leaving the others talking as long as at least one of the other parties possesses supervision on their connection.

Telecommunicators shall be able to mute any participant in the conference and shall be able to exclude any participant from hearing other parties in the conference to allow for private consultation.

The status of the call shall be presented visually in a window that also shows the status of all other calls at the workstation (active, abandoned, on hold).

Callback

The workstation shall have the ability to callback a 9-1-1 caller by dialing the ANI received during the 9-1-1 call setup.

The workstation should provide a single feature key to perform this operation. Manual dialing of the number by the telecommunicator shall not be necessary.

The callback of emergency TDD and wireless calls should be performed in the same manner.

Hold

The answering position must allow the telecommunicator to place up to five 9-1-1 or administrative calls on hold with a single keystroke or mouse click.

The system must store the ANI/ALI information while the call is on hold, hence avoiding repetition of the ALI request.

Forced Disconnect

Telecommunicators shall be capable of releasing an existing 9-1-1 call at any time, regardless of whether the calling party has hung up.

Muting

Telecommunicators must have the ability to block a caller from hearing and talking with the remaining parties in the conference.

Monitor

Any authorized telecommunicator or supervisor must have the ability to silently listen to another telecommunicator's telephone conversation from his/her workstation. Such action must not cause any audio or visual disturbance at the monitored answering position.

Barge-In

The workstation shall give the Telecommunicator the ability to barge into an existing call by clicking on the appropriate circuit indicator on their screen or pressing the appropriate line appearance on the telephone.

Upon entering any 9-1-1 or administrative call for which ANI/ALI or Caller-ID information is available, such information shall be immediately displayed on the telecommunicator's display.

Recommended Spares

The vendor shall provide a list of recommended spares.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

Interfaces

Given the mission-critical nature of the system and the various interfaces that need to be supported now or in the future, the following interfaces must be supported. If any interface requires additional software, hardware, or external devices please describe specifically.

- CAMA analog
- CAMA T1
- T1 CAS
- ISDN PRI
- ISDN Clear Channel
- SS7
- SIGTRAN (SS7 over IP)
- SIP (VoIP)
- H.323 (VoIP)
- SNMP
- Diameter

Vendor shall describe the design of the interfaces and any additional interfaces required, or supported, by their proposed solution.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

System Availability

It is a requirement that the system deliver an industry standard up time of 99.999%. The proposer must describe any predictable maintenance or upgrade process affecting hardware, firmware, or software that would require the proposed solution to be removed from service for any length of time.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

Redundant Configuration

The system shall support installation in a dual redundant configuration. In a dual redundant configuration, redundant functionality resides at two physically distinct locations. The two locations are connected to each other via an IP Network which may be provided by agency or may be part of a larger vendor proposed solution. The Central Equipment at either location shall be fully capable of supporting all positions at all agency locations. Each location shall have local survivability such that if one location becomes completely unavailable due to a catastrophic natural or man-made event, the second location can continue to process 9-1-1 calls.

Vendor shall describe the call flow in the event that the Main ECC should suffer a catastrophic failure.

Vendor shall describe the network bandwidth and latency requirements necessary to support the dual redundant configuration.

Vendor shall describe whether they are proposing a hosted solution (maintained wholly offsite from the ECC, in vendor provided facilities), a Customer Premise Equipment (CPE) based solution, or a hybrid. Vendor shall then describe the redundancy of the proposed solution and

the logical and physical components of the redundant architecture.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

Future Proofed Architecture

The system shall be designed to future-proof against the requirement for a 'forklift' upgrade at any time during the transition to NG9-1-1. In essence, the ECC seeks an Evergreen IT Environment. "Evergreen IT refers to running services comprised of components that are always up to date. Evergreen IT encompasses not only the services at the user level, but all of the underlying infrastructure, whether onsite or outsourced."[54]

Additionally, "Evergreen IT is the perpetual migration of end-user software, hardware and associated services such as mailboxes, telephony, file storage and the infrastructure supporting the technology. It requires a combination of people, process, and technology to deliver optimal results and involves a budgetary and executive commitment to ensuring that no end-user technology is ever more than N-x (x to be defined by each organization) behind the currently available version within a pre-determined timeframe.

For hardware, it means that every piece of physical equipment is kept within warranty or lease and is refreshed on a fixed timeline. The process means that the organizational processes are in place for procurement, licensing, scheduling, communications and deployment are in place and highly repeatable. For this, creating a set of tasks that are repeatable and in constant use will be vital, or as Gartner Analyst Kleynhans puts it, enterprises much have a production-line model of dealing with change.

"With regards to technology, this means that the information required to trigger an evergreen event such as a hardware replacement or software upgrade is continually available and updated. Additionally, the technology systems to support the processes identified earlier exist and are understood by every team that interacts with them. The goal is that a real-time understanding of the IT environment and its currency is always available, and that for all hardware or software that is outside of the defined evergreen thresholds, a project is running to perform the upgrade."[55]

The vendor shall provide a detailed response as to how they provide an Evergreen solution. If the vendor does not offer this option, they shall explain any requirements to add equipment, firmware, software, services, or technical capabilities in order to facilitate the solution as required by this RFP. In addition, the vendor shall provide any additional elements or implementation details required to support interoperable, multimedia capable, NG9-1-1 services. If there is any cost associated with such additions, they must be identified in this proposal. The vendor will be expected to absorb any additional costs not identified in the proposal but required in order to facilitate a fully capable NG9-1-1 system as defined in this RFP.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

Multimedia Requests for Emergency Assistance

As part of the evolution of 9-1-1, new call types will be part of an NG9-1-1 world. These new call types are referred to as 9-1-1 Requests for Emergency Assistance (RFEAs), depicting they are no longer simply voice oriented calls. The agency intends to be able to handle RFEAs in the future and this solution must be capable of supporting these types of transactions between the public and the ECC. Put more succinctly, it is mandatory that the system architecture support RFEAs. We understand that some additional components such as servers and/or software modules/updates may be required. These components, along with any other solution elements required to support this functionality, must be specifically identified in the solution and must be included in initial pricing. Failure to account for these items in both the detailed design and price quote will result in disqualification of the vendor.

Describe how your system supports multimedia RFEAs now or how it will in the future. Please describe any industry testing for such RFEAs you have participated in and describe any prototypes that have been developed to support RFEAs.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

Virtual ECC and Remote Positions

It is the agency's desire to have the option to allow telecommunicator positions to securely access the system in a "Virtual ECC" environment wherein login would place virtual positions into a group of operators specific to an identified ECC. This applies to a number of scenarios including, but not limited to, field/tactical dispatch and emergency relocation of ECC personnel and/or equipment.

Vendor shall describe how the system supports the implementation of a Virtual ECC.

The system shall support the deployment of remote positions at a location to be determined either ahead of any planned deployment or "on the fly" in the event of a major incident requiring tactical dispatch capabilities closer to the scene. The agency will supply the IP transport network between the ECC and the remote positions, if an ESInet is not already in place to support said transport. The remote positions shall have the same functionality and access to resources as the local positions.

Vendor shall describe the network bandwidth and latency requirement per position. Vendor shall also describe any additional data or networking equipment required at the remote position location or at the primary location to support this function.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

Interoperability

As previously defined, any proposed system shall support the capability of ECCs to receive 9-1-1 Requests for Emergency Assistance and related data such as location information and callback numbers from the public, then process and share the 9-1-1 Requests for Emergency Assistance and related data with other ECCs and emergency response providers, regardless of jurisdiction, equipment, device, software, service provider, or other relevant factors, and without the need for proprietary interfaces.

In addition, vendor shall describe the programs it is participating in to test their system with products from other vendors to support this interoperability. It is expected that the selected vendor will be able to demonstrate interoperability between multiple agencies, in a multimedia, IP-based environment as a condition of award.

Vendor shall describe if its proposed solution utilizes open source software/products and detail what, if any, are utilized. Describe how product enhancement control is maintained independent of open source community advances. Describe any risk associated with utilization of open source software. If the vendor utilizes any Application Programming Interfaces (APIs) such use must also be identified in the vendor response to this section. The agency encourages the use of open APIs wherever possible and practical provided they can be implemented in secure fashion. In the event the vendor utilizes or relies on APIs that are proprietary, that information must also be disclosed, and described, in this section of the response.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

Ability to Support Multi-agency Solution

Many agencies are now seeking a multi-agency solution. In short, this means that the agency needs the core system to do things at a general level (as previously noted and described), but they also need functions that are unique to the local level.

The vendor shall explain how their architecture supports multiple agencies, including core and distributed architectures, and provide detailed information on both technical function and integration of unique local business rules and needs within the same system in a shared environment.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

Automated Call Distribution (ACD)

The system must be equipped without additional cost to provide functional equivalent to a legacy ACD. The following functional capabilities for routing calls internal to the ECC are required:

- Ring All
- Ring All with Conference (Rings all telecommunicators. As each answers, they are joined in the conference)
- Priority (Round Robin)
- Longest Idle

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

Fault Tolerance

The system must be designed so that no single point of failure exists. Whether hosted or premise-based, the system must be fault tolerant and this capability must be proved by the vendor. The Bidder shall describe their system architecture with respect to the major components or modules and describe how the system will react to a failure of each major component or module. To reiterate, regardless of architecture, the system MUST NOT contain a single point of failure.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

Power Distribution

If there are premise-based components to this solution, not including standard workstation equipment which is covered separately, power must be delivered to the Central Equipment such that the failure of a single power feed will not result in the loss of more than 50% system capacity.

Should the vendor propose a hosted solution, vendor must be prepared to demonstrate, via detailed documentation and real-world demonstration, the redundancy and resiliency of their system to include geographic and network diversity.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

Interface Design

Given the mission-critical nature of the system and the various interfaces that need to be supported now or in the future, the following interfaces must be supported. If any interface requires additional software, hardware, or external devices please describe specifically.

- CAMA analog (Until full IP to ECC is delivered)
- CAMA T1 (Until full IP to ECC is delivered)
- T1 CAS
- ISDN PRI
- ISDN Clear Channel
- SS7 / Diameter
- SIP (VoIP)
- H.323 (VoIP)
- SNMP to/from all relevant network elements (to include ECC)

Vendor shall describe the design of the interfaces. Reliance on i3 alone will not be considered sufficient to demonstrate relevant interfaces. As with all other operational components, vendor shall be expected to demonstrate the impact of any remaining legacy elements and how vendor proposes to deliver NG9-1-1 functionality should those legacy elements remain.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

Bandwidth Requirements (ESInet or Cloud are both options)

The network between the ECC and the ESInet will need to be a private network that supports IP-based traffic and services. It must have scalable bandwidth to support emerging technologies and services.

The ESInet concept outlined in some documentation was originally conceived in the late 1990s, and while it meets some of the requirements stated above, the advent of newer transport technologies has eclipsed the need for ESInets as the exclusive network topology for NG9-1-1 solutions. ECCs should have redundant connections to whatever transport layer is selected. And the connections must be resilient, secure, diverse, and logically separated. However, many cloud architectures provide for a great deal more in the way of options, bandwidth, and security while meeting all of the fundamental needs of an ESInet. To this end, the agency will strongly consider alternatives to the ESInet concept, and encourages vendors to propose modern, scalable, secure, interoperable solutions that are not subject to proprietary implementations and afford ECCs greater economies of scale and enhanced functions. In the event there are proprietary elements to the solution, the up-front (design and development) and ongoing cost of any such element(s) must be clearly defined. Additionally, if any proprietary elements preclude, or prohibit, interoperability they will not be allowed. The vendor shall be responsible for identifying any such issues, and should they not disclose the nature and function of proprietary elements they may be disqualified from the RFP process. Should an award of contract be made to a vendor who subsequently identifies any elements of this nature after the fact, the agency shall reserve the right to cancel the contract for material breach and recoup any associated costs.

The solution shall be engineered to support real-time traffic, including data, audio, and video (multimedia) and must be interoperable.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

Direct IP Trunks

The proposed system must have the capability to terminate native IP telephony for both emergency and administrative calls. Please state if additional equipment is required to terminate direct IP trunks and provide pricing in the Options Pricing section. If Direct IP trunking is not available, or not interfaced to/from ESInet to ECC, vendor shall so state. Additionally, vendor shall describe plan to provide NG9-1-1 functionality in the absence of IP trunks. Gateways are not an acceptable alternative, as multimedia capabilities are compromised.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

CAD Interface *(See CAD Section)*

Timing / Synchronization

Network Time Synchronization

The agency wishes to ensure that its servers, security systems, media recorders, and other devices are operating in sync. The existence of widely accepted protocols makes it possible to deploy a compliant system and be confident in its ability to track time as expected.

Any solution must use **Network Time Protocol**.

The NTP standard employs servers that supply clients, such as the computers in your network, with current Coordinated Universal Time, or UTC, information in response to individual requests. Although your hardware can ask for the present time from many different servers in the network, some devices provide more accurate data than others due to factors like system lag and latency.

The timekeeping servers in these networks are arranged in distinct strata, also known as layers. The most accurate devices exist in Stratum 0, and they include atomic, radio and other high-precision clocks, such as those found in NIST laboratories and GPS satellites. Stratum 1 servers, also known as primary time servers, are connected directly to Stratum 0 devices as well as their same-level peers.

This protocol also:

- Allows clients to connect to multiple NTP servers for data backups, heightened accuracy, and testing purposes;
- Corrects for communication latency and individual clock drift;
- Uses a standardized, 64-bit UDP packet that can theoretically achieve picosecond (trillionth of a second) timing and determine dates within a 136-year range; and
- Permits peer-to-peer communication, broadcasting, multicasting, calibration, and secure MD5 hash algorithms.

Precision Time Protocol is considered an enhanced function and will be looked upon favorably if offered as an integrated part of the proposed solution. However, this should be priced as an option unless it is already bundled into the provider's proposed architecture.

PTP, defined in IEEE 1588, facilitates applications where the NTP lacks sufficient accuracy. By utilizing hardware-based timestamping, it provides more accurate synchronization.

Instead of clients requesting timing information, master clocks initiate contact by sending them data that they can use to stay in sync. As a PTP grandmaster communicates with the clocks it's synchronizing, the information passing from one machine to the other gains a timestamp at each stop.

By using dedicated hardware devices, PTP networks gain the power to minimize latency that could arise as a result of unforeseen factors. For instance, timekeeping software routinely must contend with challenges like a lack of local operating system resources and unquantifiable delays in network communications.

There are numerous ways to overcome such hurdles. One widely accepted technique uses synchronization references that include highly-accurate GPS satellites.

The Global Positioning System, commonly known as GPS, does more than just let consumers find their way around during vacation road trips. This system consists of fixed constellations of special orbiting satellites that each carry:

- Stabilized Stratum 0 atomic clock hardware;
- Advanced location tracking circuitry; and
- Transmitters that constantly broadcast their position and clock time.

These satellites are all synchronized to the same time and have known locations due to their geosynchronous orbits. As a result, receivers can listen to multiple broadcast sources and use trilateration, to determine their own position and time deviation.

The agency understands that the most effective servers don't only use NTP. They're also conversant with PTP and other standards. This means that they can be integrated seamlessly into a range of network configurations.

The vendor should provide a detailed explanation as to how they enable the following functions:

- NTP and IEEE 1588 PTP client and server functionality
- GPS reference
- MD5 hash authentication
- SSH for secure communication
- IPv6 compatibility

As more operations shift to the cloud and other unique network architectures, the hardware they use must evolve as well. Especially in a mission-critical, public safety environment, the value of ruggedness can't be overstated.

Any proposed time synchronization servers must be able to withstand potentially high levels of humidity and heat in the event an air handler breaks in the middle of summer. If the agency's data center's infrastructure management systems fail, any proposed devices should be rated for a reasonably wide range of environmental and power supply conditions to ensure that unexpected fluctuations don't cause gaps in operational continuity. The vendor shall supply documentation as to how these requirements are met.

In addition, robustness isn't only physical. Reliable time servers can function properly even in the absence of satellite connections. In the event of signal loss, they use high-accuracy internal oscillators to keep counting the passage of fractional seconds. Since manufacturers calibrate these devices with great precision if a server loses source lock, the oscillator can compensate for any drift until signals from GPS satellites or other sources is regained. The vendor should provide detailed explanations as to how they handle, or do not handle, these requirements.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

Cybersecurity Requirements

Compliance with cybersecurity requirements is not optional. The vendor shall provide a detailed explanation as to how they do the following:

Network Security

All network interfaces connected to either a managed Wide Area Network (WAN) or protected via a Virtual Private Network (VPN) through either an ESInet, alternative transport network, or protected and discreet segment of the public internet must include protection against security attacks from all threats, both internal and external.

A robust cybersecurity plan must be in place and provided by vendor prior to award. This plan must include details as to security protocols and interfaces. If additional hardware or software is required, this must be included in the core bid, not priced as an option. Detailed pricing for security is required.

It is expected that the vendor will meet all basic security requirements as noted in the APCO cybersecurity document located here:

https://www.apcointl.org/~documents/report/cybersecurity-attacks-detection-and-mitigation

TDoS Detection and Mitigation

This type of attack targets an ECC's phones. A TDoS attack is a flood of unwanted, malicious inbound calls. The calls are usually into a contact center or other part of an enterprise, which depends heavily on voice service. The goal of this type of attack is to overwhelm the phone system with calls. TDoS attacks vary in complexity. In the simplest form, TDoS attacks come from one single contact point that may or may not utilize a spoofed number. This type of attack is most effective against smaller agencies since it does not take a substantial number of phone calls to tie up all of the phone lines. However, recent events have demonstrated that with relatively little sophistication, and only moderate resources, a TDoS attack can impact large ECCs as well. Regardless of the complexity of the attack, if the volume of phone calls is significant enough, any TDoS event can tie up resources making it difficult not only to locate the source but to also identify and process legitimate requests for service. More complex attacks employ sophisticated spoofing technology with calls appearing to originate from all over the country.

Understanding that prevention and mitigation of a TDoS attack is not an easy task, the vendor shall provide a detailed explanation of how they handle TDoS events to include prevention, mitigation, response, and recovery.

The vendor shall provide an emergency contact list for all potentially impacted systems available to the ECC that is kept updated at all times.

Vendor Response / Explanation: _____

Intrusion Detection and Prevention

Implement Intrusion Detection and Prevention System (IDPS) Capabilities

APCO supports the concepts put forth in the FCC Task Force on Optimal PSAP Architecture (TFOPA) working group 1 (cybersecurity) report with regard to the consideration of a fully deployed, inclusive IDPS system for broadband technologies in public safety. The following excerpt is from the ***TFOPA WG1*** second report:

> *The Emergency Communications Cybersecurity Center (EC3)*
>
> "As part of the initial, approved, report submitted to the Commission, WG1 determined that an additional element should be introduced into the recommended future architecture. As a result, a logical architecture was developed to illustrate the potential functions and capabilities of this new element. The group agreed to naming this element the Emergency Communications Cybersecurity Center, or EC3. The intent of the logical architecture recommendation is to create a centralized function, and location, for securing NG networks and systems. By centralizing certain features, including cybersecurity in general, and intrusion detection and prevention services (IDPS) specifically, public safety can take advantage of economies of scale, multiple resources, and systems and best practices which may already be in place or at a minimum readily available for deployment and use.
>
> "This concept is intended to empower State, local, tribal and territorial (SLTT) ECCs and 9-1-1 authority leaders, by providing cooperative options to defend both common areas of interest and individual networks and systems. Through the establishment of certain shared core services like cybersecurity, which can be utilized by multiple participating agencies, agencies can realize substantial cost savings and could also decrease the time needed to implement a comprehensive cybersecurity system.
>
> "The information collected by the EC3s that relates to the ECCs will be the result of the monitoring that the center will conduct. As a result, it will be necessary to deploy some type of sensors at ECC locations.

[Alternately, and perhaps more effectively, a way will need to be devised to get all traffic to funnel through a centralized EC3 for monitoring at a regional or State level, then aggregating the traffic of the various EC3's to, or through, a central monitoring facility. This would best be accomplished via the ESInet architecture with partnerships at the Local, State and potentially Federal level.]

> *Proposed Approach for IDPS in the NG9-1-1 Environment.*
>
> "In the proposed NG9-1-1 architecture, the Emergency Communications Cybersecurity Center (EC3) will take on the role of providing IDPS services to ECCs and any other emergency communications service or system that would consider utilizing the centralized, core services architecture proposed. For example, not only ECCs but Emergency Operations Centers (EOCs) and potentially the Nationwide Public Safety Broadband Network operated and maintained by FirstNet, could also interconnect to the EC3 service. This approach would allow public safety to build one infrastructure and use it for many clients. This provides significant economies of scale, puts multiple Federal, State, Local and Tribal resources into the same protection scheme, and allows for sharing of data, mitigation strategies, and recovery efforts across enterprise.
>
> "The potential flow of this system would begin with the Originating Service Provider (OSP) and NG9-1-1 Core Services elements, would encompass the ESInet IP Transport network within and between disparate ECCs and would provide for monitoring of call statistics, system health, anomaly detection, data sharing, mitigation and recovery while still allowing local agencies to maintain local control of day to day operations within their specific ECCs.

> Rather than requiring ECCs to build and staff such facilities, the EC3 concept allows for ECCs from within and across jurisdictions, to interconnect to the core cybersecurity system and benefit from its capabilities, whether state, local, tribal or territorial. While not specified herein, the interconnect requirements would include cyber hygiene elements at the ECC, single user sign on and multi-factor authentication at the local level and some form of agreed upon, trusted connection (and relationship) from the local levels to the State or Regional level EC3. This architecture is also intended to represent a scalable, and customizable, approach. This means for localities with larger than average emergency communications systems (major metropolitan areas such as New York, Los Angeles, etc.) there is ample opportunity to construct a single EC3 to serve this individual customer. However, any EC3 should be designed and constructed in such a way that it will interconnect with other EC3's throughout the United States with the same functions and requirements. From the regional or State level, the information should flow to a centralized repository with adequate service capabilities to support multiple clients, and incidents, in real time."[56]

Additional information about implementation options and considerations can be found in the full TFOPA reports, and specifically in the WG1 sections, located on the Federal Communications Commission website at:

https://www.fcc.gov/about-fcc/advisory-committees/general/task-force-optimal-public-safety-answering-point

APCO highly recommends becoming familiar with the EC3 concept and proposed architecture and including requirements for full IDPS capabilities in this RFP.

Until fully implemented IDPS becomes a reality for public safety, the following high level recommendations with regard to threat detection and mitigation are offered and should also be included in any forthcoming systems requirements and requests for proposals.

Implement Threat Detection and Mitigation

Measures to detect and limit the impact of security breaches are an important component of any security plan. Consider the following best practices for detecting and mitigating threats:

- Create logs to monitor all aspects of the system including physical access, network activity, device activity, and firewall configuration. Consider system performance when setting logging parameters and collect log files in a central location to prevent unauthorized modification.
- If you are using an intrusion detection system, take the time to thoroughly understand the capabilities and limitations of the system you selected before configuring the alerts and active response rules governing its operation. Configuration rules should reflect the operating behavior of your network which may differ significantly from those of a typical enterprise network.
- ***Ensure any selected vendor, with any interconnected system, provides threat detection services and has documented mitigation plans available for your review***.

Monitor the System

Through vigilant monitoring of system parameters, you can detect security breaches earlier and take steps to limit the spread of damage. Monitoring guidelines include:

- Treat alerts from intrusion detection systems with the highest priority.
- Proactively scan the network for new hosts and out-of-date systems.
- Routinely review system logs for irregular activities. Indicators such as numerous failed login attempts, unusual credential card use, and increases in network load can provide early signs of a breach.
- Create an incidence response plan which describes the actions to be taken when system irregularities are detected.
- ***Ensure any selected vendor, with any interconnected system, provides monitoring and notification to your agency 24x7x365***.

Operate Securely

The need to address security does not end once a system has been installed but is only beginning. System monitoring, account management, patch management, and firewall maintenance are all important to operating a system securely. Whether done via an EC3-like, fully deployed IDPS, via threat detection, mitigation and monitoring (either vendor, agency, or both), or via another path, the secure operation of any public safety system is a shared responsibility that must be taken just as seriously as any other aspect of the public safety mission.

The solution provider must provide a detailed explanation of all entry points into the system, including any and all "backdoors" that were built into the vendor's (or sub-contractor's) code. If there are any entry paths designed into the system by the solution developers, the vendor must verify that they do not compromise and/or violate federal IT security requirements. While the existence of these backdoors is not disqualifying (provided they do not violate Federal, State, or Local security requirements) the agency does need to know all about them in order to better protect its end of the system(s).

Vendor Response / Explanation: _____

Identity Credentialing and Access Management (ICAM)

Vendor Access

In today's environment, virtually all organizations have networks, systems, and facilities that rely on outside vendors for service. Vendors might require physical access, dedicated remote network access, network cloud access, or any combination of the three. When using a vendor, a level of risk is inherent in the relationship.

Vendors can be a service division of the product manufacturing company (e.g. Cisco Corporate Support Team supporting Cisco Networks and Hardware). Vendors can also be third-party equipment agnostic, supporting multiple platforms. Prior to granting system access to a vendor, a thorough screening and contract process should be completed. Policies are normally contained within vendor contracts.

Risk Management should be employed to negate as much risk as possible. A fine line exists between risk to the agency and the level of access required for the vendor to complete its assigned tasks. Remote access to the network can be accomplished through either a Secure Shell (SSH) Tunnel, a Virtual Private Network (VPN) or dedicated point to point line. This access can increase risk to the network if security patches are not kept up to date.

The vendor staff should also be taken into consideration. Vendor staff should meet your agency security and background check requirements. Employee continuity is very important, and several questions should be asked when negotiating with a vendor. Should a vendor's employee leave their employ, does the vendor have the ability to continue support? Is the support documentation available to more than a single employee? Is the vendor company stable and financially sound? If the vendor were to go out of business, how would this affect your agency?

When a vendor accesses your agency network regardless of the method (tunnel, VPN, point to point, cloud) a strong password policy is required. All passwords should have an expiration timeframe; the more sensitive the password, the shorter the expiration timeframe. Single use passwords for vendors are also an effective means of minimizing the risk of vendor access.

Vendor Response / Explanation: _____

Manage User Access

Secure user access is achieved through the use of authentication and authorization. Authentication is the means by which a user's identity is confirmed. Once authenticated, a user is authorized to perform certain functions as defined by their role within the organization.

- Restrict user access by capitalizing on solutions commonly deployed by IT departments, such as Central Authorization, Password Control, User Management, and Network Monitoring. Examples include Active Directory®, Kerberos, and Radius.
- Further restrict user access by establishing authorization requirements for individual devices such as routers, servers, embedded

controllers, and workstations. The type of device will dictate the best approach.
- Consider stronger authentication methods for critical host devices such as:
  - Smart Cards or USB tokens;
  - Biometric Authentication limiting access based on a physical or behavioral characteristic such as a fingerprint; and
  - Two-Factor Authentication limiting access to users with both a password and a physical token.

Vendor Response / Explanation: _____

Restrict Remote Access

Providing access to remote users presents a unique set of security challenges. Addressing these challenges requires building additional protections into the network infrastructure. Even then, remote access should only be considered for systems that already have sufficient protection against external threats. Best practices for providing remote access include:

- Use a secure connection, such as a VPN, which provides encryption and authentication of remote sessions.
- Use secure protocols and applications such as HTTPS, SSH, and SCP/SFTP whenever possible and avoid Telnet and FTP.
- Evaluate the risks associated with SNMP (Simple Network Management Protocol) before incorporating it into your design. When using SNMP, limit access to authorized system administrators with known IP addresses.
- Restrict remote access by using Two-Factor Authentication and by limiting access to required users only, such as system operators.
- To provide public access to information, create a demilitarized zone (DMZ), place a server within the zone, and mirror the required information onto the server.

Vendor Response / Explanation: _____

How does the proposed system comply with the recommendations made for cybersecurity considerations in the Federal Communications Commission (FCC) Task Force on Optimal PSAP Architecture (TFOPA)?

Vendor Response / Explanation: _____

Vendor shall provide documentation about all cybersecurity testing within their system (i.e., PEN testing, vulnerability scans, etc.).

Vendor Response / Explanation: _____

Network-based Information Technology Systems

Network-based systems (i.e., CAD, email, etc.) which communicate with other systems or devices are typically connected to the public network which makes them especially vulnerable targets. The vendor shall detail how they monitor and recognize service interruptions or abnormal system behavior and whether the interruption or behavior is believed to be the result of a cyberattack.

Vendor must provide detailed response as to how they comply with the following requirements:

- If email is accessible via CAD workstations, vendor must provide details as to how they secure each workstation and any mitigation tactics, techniques, and procedures (TTPs) that are in place to minimize risk.
- Minimize the number of users with administrative privileges.
- Implement a strong password policy; use unique passwords for each account.
- Implement weekly vulnerability network scans.
- Routinely audit user access lists; remove previous employees; confirm new users immediately at direction of ECC (if ECC administrator is not allowed to do so).

Vendor Response / Explanation: _____

Geographic Information System (GIS)

These systems are a method of accessing the ECC. It is not unusual for GIS or resources to be shared amongst several ECCs which brings a greater vulnerability and level of exposure to those connected agencies. GIS components should be isolated and not directly exposed to open networks such as the internet. The vendor shall provide a detailed response as to how they comply with the following requirements:

- Limit access to systems that access your GIS;
- Limit software applications on systems that access your GIS;
- Ensure strong password policies are in place; and
- Use unique passwords for each account.

Vendor Response / Explanation: _____

Network Infrastructure

The network is the conduit that allows information to flow among the ECC, enterprise systems, and the outside world. Intruders able to tap into the network can disrupt the flow of information. The vendor shall describe how they comply with the following requirements:

Limit Network Access Points

- Isolate the ECC system(s) as much as possible. Locating it on a virtual local area network (VLAN), for example, ensures that building traffic, including broadcasts to all nodes, remains within the logical boundary established.
- Think carefully before granting outside access. Each network entry and exit point must be secured. By granting access only when a valid reason exists, you can minimize risk and keep security costs down.

Vendor Response / Explanation: _____

Use Firewalls to Control Access

Firewalls contribute to security by controlling the flow of information into and out of network entry points. Using a set of user-defined configuration rules, a firewall determines which traffic will be allowed to pass through and onto the network. Traffic that doesn't satisfy the configured rules is rejected.

The vendor shall explain in detail how they implement best practice as applied to firewalls in their solution network design. Does the vendor place a firewall at every transition point into or out of the network? If so, describe. If not, explain why and what the alternative security solution is.

Vendor Response / Explanation: _____

Manage User Access

Secure user access is achieved through the use of authentication and authorization. Authentication is the means by which a user's identity is confirmed. Once authenticated, a user is authorized to perform certain functions as defined by their role within the organization. The vendor shall explain how they comply with the following requirements:

- Restrict user access by capitalizing on solutions commonly deployed by IT departments, such as Central Authorization, Password Control, User Management, and Network Monitoring. Examples include Active Directory®, Kerberos, and Radius.
- Further restrict user access by establishing authorization requirements for individual devices such as routers, servers, embedded controllers, and workstations. The type of device will dictate the best approach.
- Utilize potentially stronger authentication methods for critical host devices such as:
  - Smart Cards or USB tokens
  - Biometric Authentication limits access based on a physical or behavioral characteristic such as a fingerprint.
  - Two-Factor Authentication limits access to users with both a password and a physical token.

Vendor Response / Explanation: _____

Remote Access

Providing system access to remote users presents a unique set of security challenges. Addressing these challenges requires building additional protections into the network infrastructure. Even then, remote access should only be considered for systems that already have sufficient protection against external threats.

The vendor shall provide a detailed explanation as to how they comply with the following requirements:

- Use a secure connection, such as a VPN, which provides encryption and authentication of remote sessions.

- Use secure protocols and applications such as HTTPS, SSH, and SCP/SFTP whenever possible and avoid Telnet and FTP.
- When using SNMP, limit access to authorized system administrators with known IP addresses
- Restrict remote access by using Two-Factor Authentication and by limiting access to required users only, such as system operators.
- To provide public access to information, create a demilitarized zone (DMZ), place a server within the zone, and mirror the required information onto the server.

Vendor Response / Explanation: _____

In addition to detailed answers to the previous requirements, the vendor shall provide a detailed response as to how they accomplish the following:

- Choose devices and protocols that support encryption, integrity, and nonrepudiation whenever possible. Encryption protects the information traversing a network by making it unreadable to unauthorized users. Integrity checks determine if any changes have been made to a network message. Nonrepudiation verifies the identity of an information source.
- Give preference to devices with logging capability. Event logging is available in a wide range of devices including routers, firewalls, backup systems, and access control systems. Logs can aid in early threat detection by recording significant network events, changes to firewall configuration, or user access to an area or device. Syslog is a logging standard that can be used to consolidate log information from multiple devices on a network.
- Look for tamper proofing, built-in locks, and other access control features when selecting mission-critical components.

Vendor Response / Explanation: _____

Configuring Security Features

Proper configuration of the security features of each system component is critical to adequate protection. Configuring firewalls, hardening system devices, configuring user accounts, and enabling threat detection are all tasks that contribute to secure system installation.

Configure Firewall Rules

Firewalls use a set of rules, established by the user, as the basis for determining which traffic is allowed to pass in or out of the network. For example, a rule might block all access to a specific IP address or port. Proper configuration of firewalls is essential to securing the network and should only be performed by experienced personnel. Best practices for configuring firewalls include:

- Use a combination of rules to both permit authorized traffic and deny unauthorized traffic.
- Create rules that explicitly deny access. Add rules to permit only the required access. Add a broad-based rule to deny access to all remaining traffic
- Confirm that the firewall can detect TCP "SYN-flood" attacks by tracking the state of a TCP handshake (stateful firewall).
- Include rules to restrict outbound network traffic in order to minimize the spread of damage in the event of a breach.
- Harden System Devices. By taking steps to harden System devices, you can close potential points of access into the ECC and reduce the risk of an internal attack. The hardening process varies depending on whether the target is an embedded device or an off-the-shelf Windows or UNIX®/Linux® based computer running host software.
- Evaluate each device to determine what ports and services are available. Whenever possible, disable any that do not have a planned use. Port scanning applications can help expedite the identification process. Be sure to disable ports and services that were used temporarily for device commissioning but won't be needed during operation.
- Removable media, such as USB memory sticks and compact discs, are often the source of malicious software. The safest solution is to prevent the use of all removable media, by mechanically blocking ports, for example. For those applications where removable media is necessary, take measures to restrict port access and enforce media checking procedures (i.e. anti-virus scans).

- Enable the security features built into each device including encryption, firewall capability, access control, intrusion detection and prevention, and user authorization.

Vendor Response / Explanation: _____

Host Devices

- Install anti-virus software from a reputable vendor (i.e. Symantec, McAfee, Webroot, etc.) and enable its automatic update features.
- Install and configure firewall software.
- Enable automatic operating system updates. Centrally managed updates are preferable.
- Configure User Accounts User accounts establish access levels to the domains within a system. Best practices for configuring user accounts include:
  - Replace all default vendor passwords with strong alternatives (twelve characters minimum with a mix of letters, numbers, and symbols). Likewise, remove all default logins (i.e. administrator) and system IDs.
  - Disable every user's access to the system by default and add permissions only as required.
  - Restrict each group of users to the lowest level of privileges necessary to perform their role.
  - Prevent duplication of passwords across multiple sites.
  - Use expiration dates to require users to periodically change passwords.

Vendor Response / Explanation: _____

Enable Threat Detection and Mitigation Measures

Define and describe any Threat Detection and Mitigation measures employed by the vendor. In addition, provide specifics as to how the following are accomplished:

- Create logs to monitor all aspects of the system including physical access, network activity, device activity, and firewall configuration. Consider system performance when setting logging parameters and collect log files in a central location to prevent unauthorized modification.
- If you are using an intrusion detection system, take the time to thoroughly understand the capabilities and limitations of the system you selected before configuring the alerts and active response rules governing its operation. Configuration rules should reflect the operating behavior of your network which may differ significantly from those of a typical enterprise network.
- Conduct system monitoring, account management, patch management, and firewall maintenance.
- Monitor the system to detect security breaches earlier and take steps to limit the spread of damage. Monitoring guidelines include:
  - Treat alerts from intrusion detection systems with the highest priority.
  - Proactively scan the network for new hosts and out-of-date systems.

Vendor Response / Explanation: _____

Manage Security Patches

Security patches provide protection against the never-ending flow of new threats. A good patch management plan combines policies, procedures, and qualified personnel in an effort to close security gaps without major disruption to the system.

The vendor shall describe how they comply with the following requirements:

- Take Inventory: Make a list of the devices that will require periodic security updates. The list should include network devices such as routers, firewalls, and VPN concentrators, as well as application and operating system software. An annual report on data breaches, a subset of the overall security landscape, highlights the importance of system monitoring.
- install and maintain all product specific firmware updates, service packs, and hot fixes.
- Whenever possible, use patches with digital signatures. A digital signature validates a patch's source and integrity.
- Stay up to date on newly released patches and vulnerability reports. Develop a plan for installation. A patch installation plan should include the following:

- Use a method of prioritizing patches. Most patches are routine updates that can be implemented according to a schedule. Others require immediate action to close a critical gap in security.
- Pre-approved patch installation tools that provide change management and security audit features.

Procedures for vendor certification of patches, testing of patches prior to installation, and a staged installation process to minimize the risk of disruption from the change are required. Vendor shall provide details as to how they comply.

Signed security patches should be verified just prior to installation to ensure that they have not been tampered with internally. The vendor shall develop a Backup and Recovery Plan. The plan should identify responsible parties, list the items to be backed up, and provide specifics such as backup intervals, locations, and number of versions to retain.

Vendor Response / Explanation: _____

What to do After an Attack

Vendors shall have a plan for maintaining the ability to function while the issues involved in any cyberattack are addressed. That plan must be shared with the ECC and should be kept up to date, and available, at all times. Incidents impacting either the ECC directly, or the vendor and other customers must be reported to the ECC immediately. Of particular concern are any incidents which:

- May impact national security, economic security, or public health and safety.
- Affect core government or critical infrastructure functions.
- Result in a significant loss of data, system availability, or control of systems.
- Involve a large number of victims.
- Indicate unauthorized access to, or malicious software present on critical information technology systems.

Once an attack has been identified, or even suspected, a response plan must be implemented.

The vendor shall provide their cybersecurity incident response plan to the agency. This plan must include specifics as to how any and all components deployed in support of the Agency's solution will be protected in the event of an incident. The plan must also include contact information, mitigation activities and instructions, and continuity of operations planning. Additionally, the plan shall address:

- How will the response differ if an ongoing attack operating behind the scenes is discovered?
- Who is the point of contact with the vendor? First-line supervisors and PSTs will be too busy trying to keep operations running smoothly to have time to "hunt down" contacts.
- In addition to notifying the response team, what actions should first-line supervisors take at the onset/discovery of an attack?
- What are the procedures for activating additional personnel to respond to the center?
- Is an alternate/backup solution available? If so, is it likely to be affected by the same attack or will it likely be available for use?
- What type of cybersecurity training is being provided to the ECC? How often is the training?

Mitigating the impact of a cybersecurity attack is heavily dependent upon the steps taken prior to the attack and as the attack unfolds. Policies and procedures must be in place guiding employees on how to avoid exposure to cybersecurity threats. However, it is equally important that any vendors and service providers take all available preventative measures, install monitoring and reporting systems, and keep the ECC aware of status at all times. In addition, a proper response plan must be available, shared with the ECC, and implemented seamlessly in the event of an incident.

Vendor Response / Explanation: _____

Overflow / Rerouting / Outage capabilities

The system shall allow 9-1-1 calls to be routed to a designated alternate location if all telecommunicators are busy. Likewise, should there be any catastrophic event, manmade or natural, that impacts the ECC, the system shall be capable of automatic transfer of calls to select backup

facilities, alternate ECCs, partner ECCs, or other designated facilities as prescribed by the agency.

The system shall provide the capability for an established 9-1-1 call to be transferred by the Telecommunicator to another ECC or some other destination to include voice ANI/ALI (or equivalent) and all call association data.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

Abandoned Call Info

Vendor must provide a method by which any abandoned calls are logged in the call processing system, and data from all abandoned calls is immediately available to the ECC for recall purposes. The solution shall capture, and store, all available information pertaining to each 9-1-1 RFEA and be accessible to the ECC management information system package for reports. This capability must be inherent in the proposed solution without the need for a separate logging and recording system. In other words, the vendor's solution must independently maintain a record of all transactions and make that data available to the ECC on demand.

The ANI of the abandoned caller must be available for viewing by the call taker, and the abandoned call must remain in queue with still active 9-1-1 calls. However, it shall be possible to sort the calls in queue to meet the requirements of ECC protocols.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

Redundancy & Resiliency

The system architecture shall be such that the failure of any one component or module will not result in total system failure, but only the loss of the equipment associated with that module. All vital system modules must be protected through the use of redundant modules to ensure single point failure tolerance. Vendor shall describe, in detail, redundant and resilient architectures whether they are premise-based, hosted (via cloud or other mechanism) or a hybrid solution. Vendor shall describe how this architecture facilitates reliability and availability and shall include continuity, backup, and disaster recovery plans.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

Fault Tolerance

The Bidder shall describe their system architecture with respect to the major components or modules and describe how the system will react to a failure of each major component or module. The system MUST not contain a single point of failure.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

Flexibility

The proposed system shall have the demonstrated ability to effectively manage and process a variety of different call formats including:

a) Traditional analog or digital telephone calls
b) Wireless calls in compliance with FCC requirements for the provision of location information
c) Voice Over IP in native format
d) Instant Messaging (IM)
e) Multimedia Messaging (MMS or subsequent new equivalent)
f) Short Message Service (SMS, "Cellular Text") to include Real-Time Text (RTT).
g) Video
h) Photos
i) Telematics, sensors, Internet of Things

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

Standards

In today's modern information and communications technology environment, standards have come to play a very different role than initially envisioned for NG9-1-1. At the same time, there currently exists no single standard, or suite of standards, that specifically address a full scale, interoperable, multimedia capable NG9-1-1 system that would meet the needs of ECCs. This is not unexpected given the ways that commercially available capabilities have leapt well ahead of NG9-1-1-focused standards development. Thus, it is advantageous for the agency to seek commercially available capabilities, as defined in commercially accepted and implemented standards such as those put out by IEEE, IETF and 3GPP, to facilitate meeting our operational needs. To this end, the agency shall require vendors to ensure their solutions are interoperable throughout the country, just like commercial technologies and public safety wireless broadband networks such as FirstNet. Conformance to standards alone does not bring the full complement of benefits to 9-1-1 Authorities, responders, and the public. Agencies, like other consumers, have a choice of vendors and expect that components selected from different vendors will reliably work together.

It is imperative that in the event of a disaster or any potential significant failure scenario, calls can be handled by any available service and that they all work the same way to minimize customization that unnecessarily drives up costs and complexity. Simply requiring adherence to a "standard" cannot, and will not, provide this level of interoperability or assurance. As a result, this RFP specifies objectives and operational needs over compliance with standards, requires demonstration of interoperability and establishes service level agreements, with penalties for lack of compliance.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

System Diagram

Vendor shall provide detailed diagrams of proposed system(s) to include any network dependencies and proposed network architecture. If ESInet is integrated with solution, appropriate logical and physical architecture diagrams shall be included.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

Logging / Recording

Consideration to the following operational aspects should be outlined and include a guarantee that the data stream is capable of being transferred or exported to commercial off the shelf technology (COTS) format (e.g., csv (comma-separated values), JPG file extension, WMV Windows Media Video, etc.). This applies to recordings, all statistical data, reporting, etc.

Central Recording

Solution must either provide for, or interface to a logging and recording solution. The logging and recording shall be provided at the network level via IP to ensure that recording takes place even if a position is logged out or is located remotely during an emergency event and does not have access to a local recorder.

The audio records shall be fully integrated with the management information system (MIS) application.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

Instant Recall Recording

The solution must provide Instant Recall Recording (IRR) functionality at all positions.

Calls should be accessible by an easy to use interface and provide for a rolling log of calls available for review. Vendor will state how IRR calls will be handled and for what interval they will be available for review.

The IRR must be IP-based and fully integrated with the MIS application.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

Backup

Backup must be done via NAS/SAN or External Hard Drive(s). Systems that use DVD-RAM DISK as archive will not be acceptable. Backup must also be performed in redundant fashion. Vendor shall provide detailed explanation of backup schema and planning.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

Playback

The system shall provide for the simultaneous playback of previously recorded audio while recording the maximum number of channels and shall not degrade recording performance.

The system must be capable of selecting multiple calls and playing them back in order of occurrence. The system must be able to reconstruct the digital time with voice files to play back an entire activity in real time.

The playback display must have the ability to view and select recordings for playback according to date, start time, channel number and name, call duration, and call notations (capable of being edited) recorded with the call.

The system must be capable of playing back silent periods and displaying the associated time and date during playback for proof of non-events.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

Quality

The system shall be able to conduct multiple simultaneous playback sessions (via multiple remote PCs) with no degradation of speed or quality of audio recording.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

Search

The system shall be capable of performing expanded searches. Preference will be given to those solutions that allow for single click viewing of a calendar display and single click selection of the desired day will result in all the calls for that day being viewable in a scrollable format and listed in chronological order.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

Security

The recording system must provide a system Log and User Log that reports all activity within the recording system. All accesses into the recording system must record the login number and what recordings were retrieved by the login number by time and date. The identification of which recording was retrieved must only be identified by a Hex code within the Log record.

The system must be able to provide and create administrative user accounts that control any access to the recorder functions and be able

to terminate that access automatically by date and time.

Playback access must be able to secure privileges by individual channel, time of day, single station access, department access, division access, data source, Log group, and length of time.

The playback retrieval software shall have the ability to verify authentication of a recording by its digital signature with the original recording secured within the recording folder.

The system must provide for the ability to redact portions of the call, either manually or automatically based on parameters determined by the ECC. This redaction capability is a requirement for compliance with various local ordinances, and State and Federal privacy laws and requirements.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

Reports / Admin

Consideration to the following operational aspects should be outlined and include a guarantee that the data stream is capable of being transferred or exported to commercial off the shelf technology (COTS) format (e.g., csv (comma-separated values), JPG file extension, WMV Windows Media Video, etc.). This applies to recordings, all statistical data, and reporting etc.

Self-Monitoring

The system must be capable of self-monitoring vital processes and sending alarms in the event of an alarm condition. The system shall notify the local system administrator and/or local maintenance and ECC management personnel upon detection of an alarm via email or other electronic notification method and give a brief description of the alarm condition.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

Remote Access

The system must provide maintenance personnel the capability to query the system locally and remotely through a secure broadband connection, preferably via a Virtual Private Network (VPN). Current system status, alarm history, user defined selection based reporting, and printing must be available.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

Alarm Categories

There shall be a minimum of two categories of alarms (major, minor) depending upon the criticality of the event.

The types of alarms are defined as follows:

Major failures are system failures that render the system completely unusable or significantly reduce system operability and are considered to be operationally unacceptable by the agency.

Minor failures are system failures that minimally reduce system operability or have little or no effect on system operability and usability and are considered to be operationally acceptable by the agency.

The system shall be capable of sending email notifications of alarm conditions to ECC maintenance personnel and management. The email notification must summarize the occurrence which triggered the alarm condition and provide current status of system.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

Reporting

The vendor shall provide a comprehensive management and statistical reporting functionality to provide the ECC management personnel with real-time and historical information. It shall be user friendly, customizable, and capable of generating reports for varying time periods. The system also shall be able to auto-schedule the generation of predefined reports. The vendor shall include one black and white networked laser printer to be used as a system printer.

As a minimum, the following information shall be readily available for reporting purposes:

- ANI / ALI
- Position answered
- Answer time
- Disconnect time
- Total count of calls, by type and class of service
- Average Call Waiting Report
- Average call duration
- Total Abandoned calls
- Calls by incoming trunk
- Calls by hour of day
- Calls answered by position
- Calls answered by all positions
- Calls answered by user ID

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

53 https://www.911.gov/pdf/National-911-Program-Profile-Database-Progress-Report-2019.pdf

54 https://blogs.technet.microsoft.com/valuerealization/2014/06/30/evergreen-itgetting-the-most-value-trends-and-insights/

55 https://blog.juriba.com/evergreen-it-concept-or-reality

56 https://transition.fcc.gov/pshs/911/TFOPA/TFOPA_WG1_Supplemental_Report-120216.pdf

Statement of Work (SOW) and Technical Details (Data System – CAD, RMS, etc.)

This section of the RFP is similar to the NG9-1-1 section but specific to data (CAD, RMS, Mobile Data, etc.) and must include details on multimedia ingress, transfer, and security. Agency may re-utilize most of the general components of the NG9-1-1 call processing system RFP or may combine the two into a single RFP. This template provides the basic format and data to proceed either way. Suggested topics include:

a. Scope of Service – Next Generation System Requirements
b. System Integration
c. Modules and Components
d. Specifics of each required System and sub-System
e. Implementation
f. Specifics as to implementation requirements, interfaces, interoperability, and future platform capabilities
g. This section should account for how (or if) the vendor plans to transfer data from the existing CAD and RMS systems to the new system. A data migration plan must be included. If there is any additional cost for this transfer of data, that cost must be detailed in the vendor's response/proposal.

The agency is interested in obtaining proposals that will be used in the selection of a vendor capable of providing an integrated system for computer aided dispatch (CAD) for law enforcement and fire/EMS services. In addition, the solution shall (or should at agency discretion) include wireless mobile CAD with Automated Vehicle Location (AVL) compatibility.

Standard state/local law enforcement operations modules include but are not limited to:

- Records Management
- Crimes Case Management
- Investigations
- Criminal activity tracking

The CAD module will need to interface with both Law Enforcement and Fire/EMS Services as well as with the NG9-1-1 call handling system and must contain a mobile data component that is capable of interfacing with public safety wireless broadband networks including FirstNet. It is desirable that all modules will be able to share common name and street address tables to ensure standardization of spelling and to eliminate duplicate person or business records.

Throughout this RFP document, distinct components of the proposed system will be referred to as "modules." For brevity, all modules of a proposed system and professional services provided will be collectively referred to as ''SOLUTION."

In the response you may substitute your own company's acronym for the proposed system and/or modules. Please make it clear what you are substituting for "SOLUTION."

The RFP is sectioned according to the major functional areas of the agency law enforcement departments, fire department, and emergency medical services where applicable. Other departments/divisions may also be involved where applicable. SOLUTION modules may or may not coincide with these major functional areas and there may be overlap between the requirements of functional areas. The RFP was designed to eliminate duplicate or similar questions and/or requirements although some may still occur.

The words "must" or "shall" in the specifications will indicate system functionality that is perceived as high priority, and the RFP will be evaluated accordingly. It does not necessarily mean that a

proposal will be rejected for not meeting each and every "must" or "shall" requirement.

The words "should," "desired," or "preferred" in the specifications indicate system functionality that is perceived to be of value to the organization, but could be sacrificed to obtain higher priority functionality.

Basic Requirements

There are certain basic requirements to be met. Failure to clearly indicate that the Respondent can meet these basic requirements may be reason for exclusion from further review.

The basic requirements are as follows. Please indicate whether your company and/or proposed system can conform, or not.

The Graphical User Interface (GUI) must run under the most current, and supported, version of the Microsoft Windows operating system (Windows), and a migration plan must be described for future versions.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

Mainframe type applications using terminal emulation on PCs will not be considered.

If SOLUTION uses a browser interface it must function properly with the latest Microsoft, Firefox, or Chrome browser version available (not Beta versions) within six months of the release of the new version.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

SOLUTION may utilize current versions of Mozilla (Firefox), Microsoft Edge, and if adequate security is detailed, Google Chrome.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

Data files or tables must be ODBC compliant, and data element references must conform to standard SQL naming conventions where applicable.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

Describe the ability of SOLUTION to restrict ODBC access to data tables and individual fields within tables by user group authority.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

Describe what ODBC drivers or third-party ODBC software will be recommended. If not ODBC compliant, please describe any similar data access methods that may be available.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

End user PCs and peripheral devices must interface to Solution via Ethernet network interfaces and TCP/IP.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

End user PCs and peripheral devices must be secured, any external connections must be protected by VPN, or equivalent, and all machines must remain current as to operating system and patched in accordance with cybersecurity requirements contained elsewhere in this document. Vendor is responsible for ensuring this is the case.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

Any switches, routers, or other peripheral devices must be secured, any external connections must be protected by VPN or equivalent, and all machines must remain current as to operating system and patched in accordance with cybersecurity requirements. Vendor is responsible for ensuring this is the case.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

The routine daily operations and maintenance of the proposed SOLUTION should be accomplished during normal agency business hours (8am-5pm, M-F). Systems requiring daily 'off hours' attended operations such as batch processing, updating, backup, or printing are not acceptable.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

Maintenance operations which may result in any system downtime must be coordinated with the agency well in advance (at least 72 hours prior) and must have management approval. Such operations will be conducted during non-peak hours only.

SOLUTION must be available 24 hours per day, 7 days per week with few exceptions. Please provide your recommendation for an automatic failover backup system if needed to comply.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

The application system tables, security tables, file backups, file restoration, and file reorganization (defrag) must be maintainable, based on security settings, by agency employees and/or agency appointed contractors.
❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

If chosen as a finalist, a Respondent must be willing and able to demonstrate SOLUTION at a location to be determined by the agency, on a date and time mutually agreed upon by the agency RFP review team and Respondent.

❏ **Comply**
❏ **Exception**
❏ **Does Not Comply**
Vendor Response / Explanation: _____

The decision of who furnishes the hardware and operating system software will be made by the agency as part of the contract negotiation process. The agency may negotiate to purchase or lease hardware and operating system software through a Respondent or a third party.

The Respondent must attach one printed example copy of the applicable company standard contracts to each copy of the RFP and an electronic copy in MS Word format (one).

System Integration

In broad terms, describe how your company can seamlessly supply the following solution modules:

- CAD for law enforcement and fire/EMS services
- Wireless mobile CAD with AVL compatibility
- Standard municipal law enforcement operations modules including but not limited to:
- Records Management
- Crimes Case Management

- Investigations
- Criminal activity tracking
- Jail Management

And integrate with these existing modules as applicable:

- Environmental Systems Research Institute Inc (ESRI) Geographical Information System (GIS) mapping modules or suitable equivalent as determined by agency.
- Mobile network used by law enforcement officers, firefighters, and EMS personnel. (If that network is not FirstNet)
- The Nationwide Public Safety Broadband Network (FirstNet)
- NCIC and applicable State level equivalent (to include Nlets)
- NG9-1-1 system
- ESInet or equivalent transport network
- Any Internet of Things (IoT) capabilities (Smart homes, devices, etc.)
- Telematics (i.e. OnStar, Bosch, etc.)
- Alarm system interfaces (e.g. – ASAP)

Note: Please base your response for interfaces on previous implementations of systems similar to the proposed Solution. Details of data formats and method of data exchange will be required.

In addition to describing any IoT capabilities, the vendor should describe any current or planned integrations with Smart/Connected technologies specific to public safety (i.e. connected vehicles, emerging smart alarm systems, smart building technologies, etc.). As NG9-1-1 systems are expected to include the ability to ingest and process multiple data streams and multiple data types, the integration of these technologies is of increasing interest to ECCs. The vendor should also provide any specifics as to how their system will analyze and process this data to assist the ECC in preventing "information overload" on agency staff.

Solution Modules and Components

List each module or component of the solution. Include the module name, a brief description, authoring vendor name, licensing structure, dependency on other modules, Warranty terms, preferred hardware platform, operating system, relationship of the module vendor to your company (i.e. established business partner, supplier, subcontractor, shrink-wrap software vendor).

The warranty period is the initial period in which any bugs, data conversion issues, or other issues with SOLUTION will be corrected free of charge and with top priority. Use the following list for your response. You may include a separate landscaped table or Excel spreadsheet to allow more space. Preference will be given to Respondents where the SOLUTION has limited third-party integration other than integration with agency applications as identified in this RFP. In other words, the agency prefers a solution that is authored, licensed and supported by a sole vendor.

Module Name
Module Description
Authoring Vendor
License Structure
Dependency Hardware Platform
Operating System
Business Relationship

Describe, in narrative format, any additional business relationships or arrangements with current agency vendors or software packages not shown in the table.

Describe in narrative format, programming languages or application generators used to develop all components of the Solution. List in table format, similar to the above, any required or recommended compilers, text editors, or other development software. You must include any up front and potential additional costs.

Describe in narrative format, any browsers that Solution can utilize if the application is browser-based.

Solution Implementation

Describe in narrative format:

- Your recommended methodology for preparing for solution implementation. Please provide a general outline of tasks/activities.
- Any compatibility issues with major anti-virus programs or other applicable software.
- Your ability to provide data conversion from the current SQL based Sleuth databases and from comma delimited files extracted by agency or contracted personnel.
- Specific and detailed information as to what system administrator and end user training is included. Please provide an outline of a typical schedule of informal, formal, and On the Job Training (OJT) for each category of person you normally train during implementation.
- Your recommendation for system administrator expertise and/or training related to operating system or hardware (for non-solution items).
- Estimated required system administrator time on task per week to support the solution. Itemize according to general tasks such as system backups, file reorganization, troubleshooting, upgrades, etc. Is a full time system administrator recommended?

Evaluation Criteria / Compliance Matrix

Describe the ability of proposed system to meet the requirements listed in the table below.

General Features and Functions

Requirement	Response	Exceptions and Additional Costs
Does the system architecture support a multi-tier / multi-layered approach? Please describe proposed solution architecture.		
Does the system provide global search functions so that users can search system-wide based on name, address, vehicle information, property, etc., based on SOUNDEX, partial and wild-card search, AND "Google-like" search?		
Does the system provide multiple levels of data security control access?		
Does solution include all necessary hardware?		
All data must be backed up using rolling backups to an offsite location. System performance must not be degraded during backups.		
Please provide a description of GIS integration.		
The system must be multi-jurisdictional, allowing call processing and dispatching for multiple agencies including law enforcement, fire, and medical responders.		
The system can be set up for a call taker / dispatcher workflow, or for one individual to fill both roles using the same screens.		
The call taker / dispatcher position is capable of being either local or remote.		
The software supports an unlimited number of call taker / dispatcher positions.		
Multiple call takers / dispatchers must be able to work on the same incident simultaneously.		
The system allows for the dispatching of units to be performed simultaneously with call taking activities.		

Requirement	Response	Exceptions and Additional Costs
As any dispatcher, call taker, or mobile unit updates a call, the information is immediately available to all stations.		
All functions are available from the call taker and dispatcher positions for field responder initiated incidents.		
A new incident can be immediately dispatched without any mandatory fields. Optionally, mandatory fields can be specified by the agency.		
The dispatch screen provides quick and easy access to all call for service (CFS) information, specifically type, nature of call, address, reporter / complainant names, and narrative.		
9-1-1 calls, upon being answered, automatically generate and populate the call entry window with all known data (e.g. address, registered name, phone number) based on the call-in number.		
The software provides a table look-up for addresses and can be configured on a screen by screen basis to force compliance with address entry as provided for in the centralized address database.		
As the call taker begins typing the incident address, a list of street name matches is offered; the call taker can select a suggested match to auto-populate.		
When possible, the City, State, and Zip fields auto-populate based on the street address entered.		
The system allows for the entry of intersections as incident addresses.		
The system automatically alerts the dispatcher / call taker of a possible duplicate call based on address data.		
When the dispatcher verifies a duplicate call, the duplicate calls are automatically linked.		
Calls for service can also be manually linked for any agency-defined reason.		
The system provides a means for specifying the beat or zone in which a call for service takes place.		
A “use caution” flag can be placed on any call for service.		
The system allows for agency defined call for service types (incident types). Default priorities can be specified.		

Requirement	Response	Exceptions and Additional Costs
The system allows for priority modifiers such as Routine, Just Occurred, In Progress, etc.		
The system provides a means for recording reporter / complainant data such as name, address, callback number, etc.		
Unlimited reporters / complainants can be added.		
Alerts triggered from any other module in the software are displayed to dispatchers in real-time based on people involved, addresses, vehicles, etc. For example, any alerts for warrant hits, sex offender status, etc. will display when a reporting party name is entered. These alerts provide links into the part of the system that they came from.		
Unlimited narrative details can be added.		
Narrative details are made available to all other stations in real time.		
The command line must allow call takers / dispatchers to quickly and easily enter commands using few keystrokes. The command line does not rely on cryptic key codes or memorizing order of information.		
The command line is dynamic: based on the command selected, only the necessary fields appear.		
The system supports both command line and point-and-click entry for all commands.		
The system supports drag-and-drop issuance of commands.		
The software provides automatic date/time stamping and user ID tracking of all call taker and dispatcher processes to track call and unit activity and all command processing.		
All call taker / dispatcher activity is logged and can be queried and/or printed.		
The CAD unit control panel allows for filters to be set, displaying just one type of unit or any combination of types (police, fire, EMS; on duty, off duty; assigned, available; etc.).		
The CAD unit control panel displays key information about each unit, such as unit type, call sign, details, incident assignment, beat, and location.		

Requirement	Response	Exceptions and Additional Costs
From the CAD system a call taker / dispatcher has access to a list of active calls and can dispatch the units to calls.		
The software provides agency-defined check-in times for officers to increase safety. This is configurable based on CFS type. When an officer exceeds the allotted time, the software provides a visual and/or audible warning alerting the call taker / dispatcher. The reminder provides an override / reset feature.		
A CAD call control panel displays active calls for service.		
The call taker / dispatcher is able to enter free-text messages from an officer in the log.		
The CAD call control panel displays key information about each call for service, such as incident number, call for service type, priority, status, assigned units, and incident address.		
Call takers / dispatchers are able to quickly dispatch units from a displayed list of available units in the call control panel.		
The software provides agency-defined dispatch timers based on CFS type and priority. The software provides a visual and/or audible warning alerting the call taker / dispatcher that too much time elapsed without assigning a unit(s) to the call.		
The software displays pre-built shift rosters and allows call takers / dispatchers to put multiple units on shift in a single command.		
The system is able to reroute a unit from one call to another in a single command and stack the original call against the rerouted unit. Stacking is unlimited.		
When a rerouted unit is cleared, the system allows for the unit to be sent back to the original call.		
The system provides the ability to exchange one unit with another, automatically recording in the log that the first unit was initially dispatched and then switched with the second unit.		
Units can be grouped so that subsequent commands apply to all units in the group.		
The call taker / dispatcher is able to enter free-text log entries for a call for service.		
The log can be queried by unit to generate a record of individual officer activity in a time period.		

Requirement	Response	Exceptions and Additional Costs
Calls can be cleared at any time, including prior to dispatch.		
A disposition or reason for clearing a call can be specified.		
The system provides the ability to view cleared calls.		
Cleared calls have the appropriate security, defined by the agency, to prevent unauthorized modification and viewing.		
The system has the ability to reactivate recently cleared calls (with the appropriate security credentials) and allow additional activity/dispatching of units to the original incident number.		
All vehicle information can be added to a call entry and it is automatically added to the master vehicle file.		
Bulletins such as BOLOs ("Be On the Look Out") and special instructions can be issued to groups of officers based on type, jurisdiction, etc.		

Security and Accessibility

Requirement	Response	Exceptions and Additional Costs
Access to each component of the software can be granted or restricted for individual users or for groups of users.		
The system tracks the individual who last entered or updated any transaction as well as the date of the modification.		
Access is verified by username and corresponding confidential password.		
Passwords are never displayed.		
Each user has only one username and password for the entire system.		
From the CAD, all other system modules (RMS, Jail, etc.) are quickly available based on permissions given. Other modules must be accessible with a single click or keystroke, without launching a separate program.		

Requirement	Response	Exceptions and Additional Costs
The system provides for multiple users to be on the system and using the same applications simultaneously.		
The system should have the ability to house and display pre-plan information regarding locations. Items such as floor plans, videos, camera displays, etc. are all desirable.		
The system shall provide advanced Run Card and Dispatch functionality such as the ability to interface to the radio system for toning, the ability to automate rip and runs, the ability to do automated paging, the ability to fax or email call close out sheets.		

CAD / RMS Integration

Requirement	Response	Exceptions and Additional Costs
The CAD system must seamlessly integrate with the Records Management System (RMS)		
The software provides a one-time, single point of data entry that allows information to be accessible from other modules in order to provide the greatest operator and system efficiency.		
The RMS must be accessible with a single click or keystroke, without launching a separate program.		
Hazards / alerts must be integrated between the CAD and RMS modules so that alerts entered in one area are available in the other.		
The CAD and RMS modules must share master databases for names, addresses, and vehicles so that records entered through CAD are added to these databases, and information from these databases added through the RMS are available in the CAD.		
The software provides the call taker / dispatcher with access to RMS information on the reporter / complainant, incident address, and any involved vehicles. This data includes outstanding warrants, case involvements, etc.		

Requirement	Response	Exceptions and Additional Costs
Call takers / dispatchers must be able to quickly and easily perform an automatic transfer of information to the RMS when needed. This transfer must not be a one-time transfer but must be kept up to date as the CAD call progresses.		
Calls for service (CFS) data must be readily available in the RMS to help officers in writing case reports. This information should include call for service type, location, complainant / reporters' names and addresses, narrative details, incident creation and clearance times, unit response times, etc.		

CAD Data Entry Requirements

Requirement	Response	Exceptions and Additional Costs
The software provides the ability to verify the quality of data entered into the database by performing immediate error checking, prohibiting invalid data from being saved.		
The software provides auto-completion capability for frequently entered information; once the user begins typing his/her selection, the appropriate data is automatically populated into the record.		
Users can use the Tab key to move quickly between fields.		
Required fields are easily identified by a visual indication (such as color-coded). If a user attempts to save a record without completing all required fields, the system will notify the user of the remaining required fields.		
Spell-checking is provided.		

CAD Configurability and Supervisor Functions

Requirement	Response	Exceptions and Additional Costs
The software's level of supervisor security is by user or user group.		
The software allows supervisors to maintain CAD users.		
The software allows supervisors to maintain call taker / dispatcher permissions.		
Where appropriate, fields and features can be turned on/off to best fit the agency's procedures.		
The agency staff is able to adjust commonly altered variables such as codes, tables, report parameters, etc., without the services of a professional programmer or without contracting with the bidder.		
The software allows supervisors to maintain call for service types, default priorities, and modified priorities.		
The software allows supervisors to add addresses to the master address database as necessary.		
The software allows supervisors to maintain CAD jurisdiction control information.		
The software allows supervisors to maintain officer / unit information.		
The software allows supervisors to establish beats and beat staffing plans.		
The software allows supervisors to maintain unit timers used for officer safety.		
The software allows supervisors to maintain dispatch timers used to alert call takers / dispatchers to calls waiting to be dispatched.		
The software allows supervisors to maintain lists of commonly-used unit details and locations.		
The software allows supervisors to maintain incident response codes.		
The software allows supervisors to create unlimited bulletin types in addition to the basics such as BOLOs and special instructions.		
The software provides supervisors with the ability to take over any call taker / dispatcher position.		

CAD Call Scheduling

Requirement	Response	Exceptions and Additional Costs
The software schedules calls for service for future dispatch to help manage special events, such as parades, festivals, funeral escorts, prisoner transport, etc.		
A call for service is automatically created when the scheduled activity occurs.		
Scheduled calls can be set up to notify call takers / dispatchers a specific interval before the actual event.		
When scheduling a call, the user can specify which terminal will handle the call.		
Users are warned to check the incident date when calls are scheduled for dates that are not in the near future.		
Scheduled calls can include unlimited narrative details.		
The software supports location override for scheduled calls.		
The software is able to display a list of scheduled calls, either upcoming or past.		

CAD Messaging and Notes

Requirement	Response	Exceptions and Additional Costs
The software allows instant messages to be sent to multiple recipients, such as a public message room accessible by all on-duty call takers / dispatchers and officers.		
The software allows private instant messages to be sent.		
The software can be configured to provide visual and/or audible alerts or also bring the software program to the front of the all other open windows when the user receives an instant message.		
The software allows email-style messages to be sent to multiple recipients.		

Requirement	Response	Exceptions and Additional Costs
The software allows users to store or delete received email-style messages.		
The software must log all sent email-style messages.		
Private email-style messages can be sent/received and are logged.		
The software provides a note pad function that allows call takers / dispatchers to type in any unlimited text and store the text within CAD.		
The software provides a means for leaving electronic shift notes.		
Note pad entries are stamped with the date/time and user who created them.		

CAD Mapping

Requirement	Response	Exceptions and Additional Costs
The mapping software must be tightly integrated with the CAD system and accessible with a single click from the CAD system.		
The mapping software must be based on ESRI-compatible mapping components.		
Users can choose from available data layers, such as ESNs, counties, roads, railroads, postal zones, etc.		
All dispatch functions are available from the map.		
Map functions are available from other dispatch screens as appropriate.		
The map has an integrated CAD command line.		
The map has full drag-and-drop support for issuing CAD commands.		

Requirement	Response	Exceptions and Additional Costs
Active incidents are automatically plotted on the map as they are entered, and automatically removed from the map as they are cleared.		
Key incident data is displayed, including address, coordinates, nearest intersection, incident code, priority level, and assigned units.		
Dispatch alerts (if an incident has been waiting past an agency-defined time to be dispatched) appear on the map.		
The map uses AVL to show unit locations.		
The call taker / dispatcher can filter which units to view, such as on-duty units and/or off-duty units, or by unit type (law enforcement, fire, EMS, etc.).		
Key unit data is displayed, including call number, unit type, status, etc.		
Unit alerts for officer safety checks (based on agency-defined times) display on the map.		
The map offers a routing function. Routes can be drawn between any combination of unit locations, incident addresses, and other addresses.		
Road segments can be marked as closed for routing purposes. Barriers or closed segments are displayed on the map.		

RMS Security and Accessibility

Requirement	Response	Exceptions and Additional Costs
Access to each component of the software can be granted or restricted for individual users or for groups of users.		
For each component, access levels include view, edit, print, delete, admin, etc.		

Requirement	Response	Exceptions and Additional Costs
Access is verified by username and corresponding confidential password.		
Passwords are never displayed.		
Each user has only one username and password for the entire system.		
From the RMS, all other system modules (CAD, Jail, etc.) are quickly available based on permissions given. Other modules must be accessible with a single click or keystroke, without launching a separate program.		
The system tracks the individual who last entered or updated any transaction as well as the date of the modification.		
The system provides for multiple users to be on the system and using the same applications simultaneously.		

Integration Between Modules

Requirement	Response	Exceptions and Additional Costs
The RMS system must seamlessly integrate with other software modules (CAD, mobile CAD/RMS, Jail, etc.).		
Full integration must include automatic, seamless transfer of critical information between software modules. Examples include: • transfer of CAD incident information to RMS • transfer of hazard information on names and addresses to alert call takers / dispatchers of potentially threatening situations for officers • transfer of arrest data from RMS to the jail booking function		
The software provides a one-time, single point of data entry that allows information to be accessible from other modules in order to provide the greatest operator and system efficiency.		
Other modules (CAD, Jail, etc.) must be accessible with a single click or keystroke, without launching a separate program.		

Requirement	Response	Exceptions and Additional Costs
Hazards / alerts must be integrated between the RMS and CAD modules so that alerts entered in one area are available in the other.		
The RMS and other modules must share master databases for names, addresses, and vehicles so that records entered through RMS are added to these databases, and information from these databases added through the other modules are available in the RMS.		
Call takers / dispatchers must be able to quickly and easily perform an automatic transfer of information to the RMS when needed. This transfer must not be a one-time transfer but must be kept up to date as the CAD call progresses.		
Call for service data must be readily available in the RMS to help officers in writing case reports. This information should include call for service type, location, complainant / reporters' names and addresses, narrative details, incident creation and clearance times, unit response times, etc.		

RMS Data Entry Requirements

Requirement	Response	Exceptions and Additional Costs
The software provides the ability to verify the quality of data entered into the database by performing immediate error checking, prohibiting invalid data from being saved.		
The software provides auto-completion capability for frequently entered information; once the user begins typing his/her selection, the appropriate data is automatically populated into the record.		
Users can use the Tab key to move quickly between fields.		
Required fields are easily identified by a visual indication (such as color-coded). If a user attempts to save a record without completing all required fields, the system will notify the user of the remaining required fields.		
Spell-checking is provided.		

RMS Configurability and Supervisor Functions

Requirement	Response	Exceptions and Additional Costs
The software's level of supervisor security is by user or user group.		
The software allows supervisors to maintain RMS users.		
The software allows supervisors to maintain user permissions.		
Where appropriate, fields and features can be turned on/off to best fit the agency's procedures.		
The agency staff is able to adjust commonly altered variables such as codes, tables, report parameters, etc., without the services of a professional programmer or without contracting with the bidder.		
The software allows supervisors to maintain name, address, and vehicle alert types and permissions for each based on user or user group.		
The software allows supervisors to maintain a list of case report types (patrol, investigations, narcotics, juvenile, etc.) and permissions for each based on user or user group.		
The software allows supervisors to maintain a list of case dispositions and whether each disposition closes the case.		
The software allows supervisors to maintain a local ordinance list.		
The software allows supervisors to maintain case printing formats (such as an internal report, a media report, a state's attorney report, etc.).		
The software allows supervisors to maintain an unlimited list of "other" case involvement types (mentioned, driver of vehicle, owner of vehicle, family member, etc.).		
The software allows supervisors to maintain the system's case management system.		
The software allows supervisors to maintain a list of the agency's property / evidence shelves, lockers, bins, etc.		
The software allows supervisors to maintain parking ticket status options and adjustable / sliding parking ticket fee schedules based on ticket age.		

CAD Reporting

Requirement	Response	Exceptions and Additional Costs
An incident summary printout or cover sheet is provided.		
The call for service list can be queried, filtered, sorted, and printed.		
The log of call taker / dispatcher and officer activity can be queried, filtered, sorted, and printed.		
The software provides a report generator for building custom statistical and analytical reports. The report generator is provided by the same vendor (not third-party).		
Access to the report generator is permission-based by user or user group.		
The report generator allows users to include in a report any data entered into the CAD system.		
The user has control over layout decisions such as field arrangement, column width, label text, font size, line spacing, etc.		
Data on reports can be grouped or sorted by any data element.		
Data can be filtered to create a report of incidents in a specific beat of a specific call for service type in a specific date range, for example.		
Multiple data filters can be applied using and/or logic.		
The reporting system supports ad-hoc queries.		
The reporting system includes "Google-like" searching of narrative fields.		
The system supports crime analysis and data-driven policing.		
The system allows for statistical analysis and comparison of data over time periods, between areas, etc.		
Reports can be easily printed or emailed in a professional-looking format.		
Reports can be exported to PDF or Excel.		
When creating a report, the user can choose which users can access, run, or modify the report.		

Requirement	Response	Exceptions and Additional Costs
Reports can be saved and easily modified at a later time.		
The system provides for recurring reports to be scheduled and uploaded to a file share or emailed to specified users.		
The reporting system is COMSTAT compatible.		
Available data for reporting includes, but is not limited to: • incident date / time data, including date, time, year, month, week, day of week, quarter, hour of day, etc. • the name and information about the call takers / dispatchers who handled the call • call for service number • call for service type / incident code • reporting method (9-1-1, 10-digit number, walk-in, etc.) • data from associated case such as case number, primary officer, etc. • incident address • narrative details • unit response times (assigned, enroute, arrived, cleared)		
A user with sufficient permission is able to generate a variety of reports including at least the following: • Area / section activity report • Call for service priority analysis • Daily or shift-based call for service summary • Call for service breakdown by month, by day of week, by hour of day • Call for service breakdown by nature of call • Call for service breakdown by source, by disposition • Call for service breakdown by station, by call taker / dispatcher • Response time analysis by area, section, priority, etc. • Summary of activity for an address or business name • Unit assignment report		

RMS Reporting

Requirement	Response	Exceptions and Additional Costs
The software provides professional-looking case report printouts. The agency can define which case components are printed and create case printing defaults, such as an internal report, a media report, a state's attorney report, etc.		
The case report list can be queried, filtered, sorted, and printed.		
The software provides a report generator for building custom statistical and analytical reports. The report generator is provided by the same vendor (not third-party).		
Access to the report generator is permission-based by user or user group.		
The report generator allows users to include in a report any data entered into the RMS system.		
The user has control over layout decisions such as field arrangement, column width, label text, font size, line spacing, etc.		
Data on reports can be grouped or sorted by any data element.		
Data can be filtered to create a report of crimes involving a particular offense in a single geographical area in a specific date range, for example.		
Multiple data filters can be applied using and/or logic.		
The reporting system supports ad-hoc queries.		
The reporting system includes "Google-like" searching of case narratives and all other narrative fields.		
The system supports crime analysis and data-driven policing.		
The system allows for statistical analysis and comparison of data over time periods, between areas, etc.		
Reports can be easily printed or emailed in a professional-looking format.		
Reports can be exported to PDF or Excel.		
When creating a report, the user can choose which users can access, run, or modify the report.		

Requirement	Response	Exceptions and Additional Costs
The system provides for recurring reports to be scheduled and uploaded to a file share or emailed to specified users.		
Available data for reporting includes, but is not limited to: • Case report data, including case number, case date and time, address, primary officer, status, nature of incident, offenses, complainants, suspects, offenders, arrestees, names of those cited and warned, victims, witnesses, other involved parties, geographical area, comments, disposition, etc. • Data on summons / citations / tickets and warnings, including violation type, issuing officer, offender name and personal data, ticket date/time, ticket number, location, jurisdiction, speed clocked, speed cited, speed limit, court location and date/time, disposition, comments / remarks, etc. • Statutes and offenses • Data on warrants, including date received, date served, date cleared, issuing judge and court, defendant name and personal data, warrant file transaction number, court warrant number, charge, status, comments / remarks, bond amount and type, serving officer, etc. • Data on parking tickets, including ticket number, vehicle data including registered owners, issued date and time, issuing officer, location, offense, comments / remarks, etc.		
A user with sufficient permission is able to generate a variety of reports including at least the following: • Daily or shift-based summary of case reports • Summary of case reports for a specified time range • Summary of case reports broken down by approval status or by disposition • Summary of case reports broken down by offense or by nature of incident • Summary of case reports by geographical area • Summary of juvenile cases • Summary of arrests broken down by officer • Summary of summons / citations / tickets broken down by officer • Officer case load report • Statistical reports of crimes within an area • Year-to-date crime totals • Comparison of crime statistics from current year to previous years • Outstanding warrants summary • Report of warrants served broken down by serving officer • Unpaid parking ticket summary • Report of parking tickets issued broken down by officer		

Requirement	Response	Exceptions and Additional Costs
The vendor must be willing to commit to state compliance for all RMS state specific requirements within a particular and negotiated time frame. Monetary incentives for compliance within the negotiated time frames is preferable.		

Master Name Record Requirements

Requirement	Response	Exceptions and Additional Costs
The software uses the master name concept to link all activity of an individual person (or business) to a single master name record.		
The master name database is shared among all software modules so that information entered about an individual through the Jail module, for example, is available in RMS.		
The software provides a listing of all activity the person was involved in, including calls for service, case reports, jail bookings, summons/citations/tickets, parking tickets, warrants, registered vehicles, etc.		
The system activity list links to any record in which the person was involved in the module it originated. Access to this data is controlled by user permissions.		
The master name record is linked from any name field anywhere in the system. This includes but is not limited to: • CAD Callers • Vehicle Owners • Complainant / Reporters • Suspects • Offenders • Arrestees • Traffic Violators • Field Interviewees • Victims • Witnesses • Warrant Names • Property Owners • Inmates		

Requirement	Response	Exceptions and Additional Costs
• Civil Process Names • Customers / Vendors • Bicycle Registrations • Sex Offenders		
The system maintains the following master name record data elements for people: • Name (first, middle, last, suffix) • Sex • DOB / Age • Address (street, city, state, zip code) with history • Telephone numbers (unlimited) • Aliases • Occupation • Ethnicity / Race • Physical description • Scars / Marks / Tattoos • ID numbers (including but not limited to driver's license, social security number, state ID, FBI number, arrest number, fingerprint classification number, etc.) • Additional agency-defined ID numbers • Education • Marital status • Religion • Citizenship • Place of birth • Unlimited mugshots • Relationship data (next of kin, known associates, employers, etc.)		
The system maintains the following master name record data elements for businesses: • Name • Type (business, religious organization, government agency, etc.) • Address (street, city, state, zip code) with history • Telephone numbers (unlimited) • Aliases • Contact person name, address, and telephone numbers • Building data (year built, square footage, maximum occupancy, etc.) • Alarm company data • Relationship data (owner, employees, etc.)		
The software eliminates the need to duplicate any information already entered.		

Requirement	Response	Exceptions and Additional Costs
Once a master name record is created, the software provides the ability to update any basic data fields and add or modify other information as available.		
The software cross-references the master name record to all other records associated with an individual.		
Names are automatically added to the master name database when entered on a record, or new names can be manually added.		
The software has built-in checking to reduce the possibility of creating duplicate master name records for the same individual.		
The software has the ability to merge duplicate name entries, giving the user the choice of which name data elements to keep for the merged record.		
The software restricts access to specific functions by user ID and password.		
The software stores narrative linked to a name and displays it upon inquiry for that name.		
The software links multiple addresses to a master name record and dates all changes to an address.		
The software associates previous address records with a date of address change, along with the person that changed the address.		
The software has the ability to check all coded entries in the master name record for validity at the time of data entry.		
The software automatically checks a name against the list of outstanding warrants and notifies the user.		
The software automatically checks a name against the list of known sex offenders and notifies the user.		
The software automatically checks a name against the list of current jail inmates and notifies the user.		
The system automatically displays any user-entered name alerts (medical alerts, officer safety threats, and other agency-defined alert types).		
Users can easily create new name alerts from a master name record.		

Requirement	Response	Exceptions and Additional Costs
The system allows searching for individuals and businesses by full or partial names.		
Searching for an alias of a master name record finds that master record.		
The software provides Soundex capabilities when searching by names.		

Master Address Record Requirements

Requirement	Response	Exceptions and Additional Costs
The software uses the master address concept to link all activity occurring at an address to a single master address record.		
The master name database is shared among all software modules so that information entered about an address through the Jail module, for example, is available in RMS.		
The software provides a listing of all activity the address was involved in, including calls for service, case reports, etc.		
The system activity list links to any record in which the address was involved in the module it originated. Access to this data is controlled by user permissions.		
The master address record is linked from any address field anywhere in the system. This includes but is not limited to: • Individual's residences • Business locations • CAD calls for service • Case reports		
The software cross-references the master address record to all other records associated with an address.		
Addresses are automatically added to the master address database when entered on a record.		

Requirement	Response	Exceptions and Additional Costs
The software has built-in checking to automatically merge differently-typed addresses the correspond to the same address (e.g. "123 Main St" and "123 main street" do not create duplicate address records).		
The software has the ability to merge address records (e.g. to indicate that "Joe's Gas Station" and "114 E Lincoln" are the same address and should be treated as such).		
The software restricts access to specific functions by user ID and password.		
The system automatically displays any user-entered address alerts (hazardous materials, alarm system, water supply information, officer safety threats, and other agency-defined alert types).		
Users can easily create new address alerts from a master address record.		
The system allows searching for address by house number or full or partial street name.		
Searching for a merged address record finds the appropriate master address record (e.g. typing "Joe's Gas Station" finds "114 E Lincoln" as in the example above).		

Master Vehicle Record Requirements

Requirement	Response	Exceptions and Additional Costs
The software uses the master vehicle concept to link all activity of vehicle to a single master vehicle record.		
The master vehicle database is shared among all software modules so that information entered about a vehicle through the CAD module, for example, is available in RMS.		

Requirement	Response	Exceptions and Additional Costs
The software provides a listing of all activity the vehicle was involved in, including calls for service, traffic stops, tow calls, case reports, summons/citations/tickets, field identifications, parking tickets, etc.		
The system activity list links to any record in which the vehicle was involved in the module it originated. Access to this data is controlled by user permissions.		
The master vehicle record is linked from any vehicle field anywhere in the system. This includes but is not limited to: • CAD calls for service • Traffic stops • Tow calls • Case reports • Summons/citations/tickets • Field identifications • Parking tickets		
The system maintains the following master vehicle record data elements: • License plate number • Plate expiration • Plate state • Plate type • Vehicle year • Make • Model • Color • Secondary color • Style • VIN • Features • Registered owners (with history)		
The software eliminates the need to duplicate any information already entered.		
Once a vehicle name record is created, the software provides the ability to update any basic data fields and add or modify other information as available.		
The software cross-references the master vehicle record to all other records associated with the vehicle.		
Vehicles are automatically added to the master vehicle database when entered on a record, or new vehicles can be manually added.		

Requirement	Response	Exceptions and Additional Costs
The software has built-in checking to reduce the possibility of creating duplicate master vehicle records for the same vehicle.		
The software has the ability to check all coded entries in the master name record for validity at the time of data entry.		
The system automatically displays any user-entered vehicle alerts (including agency-defined alert types).		
Users can easily create new vehicle alerts from a master vehicle record.		
The system allows searching vehicles by full or partial plate numbers or any other data element (e.g. red pickup trucks).		

Property and Evidence

Requirement	Response	Exceptions and Additional Costs
The software maintains information and records regarding property and evidence entered on case reports.		
All property and evidence shall be entered into the RMS only once. All categories of property shall be cross-referenced so that entry of property records will result in automatic checks of all other related property/evidence Subsystems.		
The system shall support multiple categories of property and evidence, such as stolen property reports, lost property reports, found or recovered property items, contraband or seized property items, evidence items, etc.		
The property/evidence input screens should adjust to type of property selected, listing just necessary fields for input.		
Information stored about an item of property or evidence is at least the following: item number (automatically generated by system and associated with case report number), type and subtype, make, model, color, quantity, serial number, value (estimated or known) owner, free-text comments, and current location.		

Requirement	Response	Exceptions and Additional Costs
Additional information stored about drug items includes drug type and quantity.		
Additional information stored about firearm items includes firearm type and caliber.		
Additional information stored about security items includes security type (bond, cash, check, etc.).		
A property record must provide single-click access to the associated case report.		
The system allows attaching digital photos of each piece of property / evidence to that item's record.		
The property and evidence system includes barcoding capability.		
The system provides effective inventory control of property and evidence held by the department.		
The property and evidence system must provide the functionality to capture information regarding the intake, movement, and disposition of property and evidence and must produce appropriate "chain-of-custody" reporting.		
Movement actions include transferring property internally, transferring to / receiving from personnel, and transferring to / receiving from external entities (crime labs, etc.).		
"Google-like" searching capability allows users to search for property and evidence items based on all comment and narrative fields.		
Once queried / filtered, the property and evidence list can be printed to generate reports such as property awaiting destruction, property in temporary locations, property out of agency custody, etc.		

CAD Hazards / Alerts

Requirement	Response	Exceptions and Additional Costs
Call takers / dispatchers and officers are visibly notified of any alert information for names, addresses, and vehicles involved in a call for service.		
These alerts are generated by data entered in all modules of the software (not just CAD), and the alerts provide links to the relevant data in the module from which the alert originated.		
Alerts can contain unlimited narrative text.		
Alert types can be flagged as urgent or non-urgent.		
Alerts can be deactivated if no longer relevant but will still show in the historical record.		
The software notifies the call taker / dispatcher and/or officer of any alerts for a name involved in a call for service, such as outstanding warrants, sex offender status, etc.		
Users can create other agency-defined name alerts, such as medical alerts, protection orders, etc.		
The software alerts the call taker / dispatcher and/or officer if hazardous material is stored at a site, including material name, amount, location on-site, and cutoff information.		
Hazardous material alerts provide a link to the relevant text from the Hazmat Guide.		
The software alerts the call taker / dispatcher and/or officer to protection system details for an address, such as fire alarm panel locations and sprinkler system details.		
The software alerts the call taker / dispatcher and/or officer to water supply details for an address.		
The software alerts the call taker / dispatcher and/or officer to any officer safety warnings for an address such as unlocked firearms, vicious dogs, etc.		
Users can create other agency-defined address alerts, such as known crash pads, drug sites, etc.		
The software alerts the call taker / dispatcher and/or officer to any vehicle warnings, and users can create agency-defined vehicle warnings.		

Requirement	Response	Exceptions and Additional Costs
Name, address, and vehicle alerts can be easily created during the call taking / dispatch process for future use.		
Users can be granted or denied permission to view or create specific name, address, and vehicle alert types so that these alerts can be used to store data such as confidential investigative information.		

Warrant File

Requirement	Response	Exceptions and Additional Costs
The software assigns each warrant a file transaction number or tracking number.		
The software must track information about a field identification which includes but is not limited to: • Date issued • Issuing judge • Issuing court / jurisdiction • Court warrant number • Defendant name and address • Date of birth • Social security number • Charge • Bond amount and type • Fee • Extradition radius • Remarks / comments		
The software allows users with adequate permission to change the status of a warrant for the following reasons: • Served on the person • Recalled by court		
The software maintains records on cancelled warrants for an unlimited amount of time.		

Requirement	Response	Exceptions and Additional Costs
The software provides an easily accessible warrant log that can be queried / filtered by data elements including: • Date issued • Date served • Date recalled • Warrant type • Status • Name • Address • File transaction number • Court warrant number		
The warrant log can be printed with filters applied to generate reports such as a log of all warrants issued or executed within a specified date range.		
The searchable warrant log can be quickly accessed by any user with sufficient permission, especially call takers / dispatchers, without launching a separate program.		
The CAD system automatically alerts call takers / dispatchers and officers when names with active warrants are involved in a call for service.		
The master name database flags any names with active warrants, no matter which software module it is accessed from.		

Case Reporting

Requirement	Response	Exceptions and Additional Costs
Case reports generated from calls are auto populated with data such as address, nature of the incident, complainant / reporter data, etc.		
When case reports are generated from calls for service, incident data such as responding units and unit response times is readily available to assist in completing the case report. There is no need for printed cover sheets or contacting dispatch to obtain this data.		

Requirement	Response	Exceptions and Additional Costs
Case reports can be generated without corresponding calls for service.		
The software stores basic report data such as incident date/time, primary officer, case disposition, nature of incident, location, narrative text, etc.		
A case report's disposition (status) can be updated at any time. Dispositions are agency-defined, and the case list can be queried by disposition to show a list of cases under investigation, cases sent to the state's attorney, etc.		
Multiple supplemental narratives can be added by the primary officer or by other users with the necessary permission level.		
Case narratives can include unlimited text.		
Case narratives include formatting options.		
Case narratives provide spell-checking.		
Narratives can be entered by either officers or clerks.		
Assisting officers can be added to a case report.		
Multiple specific offenses can be included on a case report.		
The software supports entering people on case reports involved with the specified offenses in the following ways: • Offender • Arrestee • Cited • Complainant • Suspect • Victim • Witness • Warned • Mentioned • Parent / Guardian • Field interviewees • Unlimited other agency-defined involvement types		
Search warrants can be added to case reports and printed in a professional-looking format.		
Unlimited case notes can be added to case reports. They are stamped with date/time and the name of the user who created them.		

Requirement	Response	Exceptions and Additional Costs
Users with appropriate permission can update and correct previously entered data on a case report.		
Files can be attached to case reports and stored on system servers, such as Word, Excel, JPG, WAV, etc.		
Attached files, when opened, are automatically launched in the appropriate application.		
Documents can be scanned for direct attachment to case reports.		
Case reports can be printed in a professional manner.		
All elements of a case report can be printed, including basic information, dispatch information, offenses, names, narratives, arrest forms, citations/summons/tickets, search warrants, field identification forms, attachments, property/evidence, etc.		
Several agency-defined case printing formats can be specified (internal report, media report, state's attorney report, etc.).		
The system allows for multiple agency-defined case report types (e.g. patrol, investigations, narcotics, juvenile, etc.).		
Access to view / create / modify each case report type is based on permissions for a user or user group.		
Cases can be easily linked or associated. For example, from an investigative report, a user has single-click access to all data in the original patrol report.		
A full audit trail shows all activity related to the case report, such as case report creation, adding and removing data, approval history, etc. Each entry includes date/time and username.		
A list of all case reports is easily accessible and can be queried, sorted, and printed.		
The case report list can be filtered or queried by data elements such as date, case report type, status, primary officer, disposition, nature of incident, names of involved parties, offenses, case number, etc.		
The system includes a "Google-like" searching capability for all narrative elements of case reports.		

Case Management

Requirement	Response	Exceptions and Additional Costs
The software includes a system for case approval.		
The system provides a means for users to indicate that they have finished work on a case report and it is awaiting approval.		
Ability to approve case reports is permission-based.		
Case approvers can easily approve a complete case or an individual component (e.g. approve basic case data or the primary narrative).		
Case approvers can "kick back" a complete case or an individual component.		
When "kicking back" a case, a field is provided for the case approver to type comments indicating needed changes.		
A case's current approval status is easily visible, and the case list can be filtered by approval status.		
Approved cases can be locked against future editing.		
Cases can be reactivated by users with appropriate permission.		
The system uses a task-based system to alert officers to cases needing their attention.		
The task system can be configured by agency administrators to match the case review and approval system the agency has in place.		
The system automatically generates tasks for the users who need to complete cases, approve cases, perform investigative review, etc. These cases are automatically completed as the tasks are finished.		
Users can manually create tasks. For example, a user can create a task for an assisting officer to add a supplemental narrative.		
Each user has quick access to his/her list of outstanding tasks or can filter the case list to show only cases he/she needs to take action on.		
Call referral forms can be added to case reports; based on user input, notification and follow up tasks can be generated.		

Requirement	Response	Exceptions and Additional Costs
The system can alert specified users when cases have aged beyond an agency-defined number of days.		
Email-style messages can be sent between users containing links to case reports.		
The case list can be queried to generate reports such as an officer's case load, a case summary for a specified date range, etc.		
Users can access a list of calls for service requiring case reports that have not yet been written.		

Arrest Records

Requirement	Response	Exceptions and Additional Costs
The system must track and maintain all information about an arrest which includes but is not limited to: • Date of Arrest • Time of Arrest • Location of Arrest • Arrest Type (on-view, etc.) • Name of Arrested Person • Arresting / Assisting Officers • Charges • Court Date / Time • Comments (unlimited)		
The software supports multiple charges per arrest entry per individual.		
Users can add an arrest record to a case report at the time of the original incident or at a later date.		
In the event of an arrest at a later date, the software has the ability to add additional supplemental narratives at the time of arrest to the original case report.		
Arrest records can be printed in a professional-looking format.		
Arrest information is available in the jail module and can be auto-populated into a booking record.		

Summons / Citations / Tickets

Requirement	Response	Exceptions and Additional Costs
The software must track information about a summons / citation / ticket which includes but is not limited to: • Ticket type (citation / warning, traffic / other) • Officer • Court and disposition data • Ticket number • Date / time issued • Offender name, address, and ID numbers • Location • Offenses • Vehicle information (plate number and state, year, make, model, color, style, VIN, registered owners, etc.) • Speed clocked, speed cited, speed limit • Narrative details and comments • Associated case report number		
Summons / citations / tickets can be associated with case reports or created without a case report.		
Summons / citations / tickets can be printed in a professional-looking format.		
A list of summons / citations / tickets is easily accessible and can be queried or filtered by data elements such as date range, offender name, ticket number, driver's license number, license plate number, etc.		
Citation list printouts can be generated with filters applied.		

Field Identification Forms

Requirement	Response	Exceptions and Additional Costs
The system allows for field identification forms for recording information about people and vehicles identified.		

Requirement	Response	Exceptions and Additional Costs
The software must track information about a field identification which includes but is not limited to: • Officer • Date and time • Identification method • Location • Name of person identified, address, DOB, SSN, etc. • Person's dress, such as gang colors • Pertinent vehicle information (plate number and state, year, make, model, color, style, VIN, registered owners, etc.) Field identification forms can be associated with case reports or created without a case report. Field identification forms can be printed in a professional-looking format. A list of field identification forms is easily accessible and can be queried or filtered by data elements such as date range, officer, individual's name, driver's license number, license plate number, etc. Field identification list printouts can be generated with filters applied.		

Offense/Incident Reporting

Intelligence Information

Requirement	Response	Exceptions and Additional Costs
System must provide for a general intelligence section that is available to all law enforcement officers as well as confidential intelligence files controlled by system securities.		
The records section must provide for capture of confidential information on persons of special interest to the agency, such as known sex offenders, habitual criminals, persons under investigation, drug dealers, etc., and produce the appropriate management reports.		

Requirement	Response	Exceptions and Additional Costs
System must Capture the following specific intelligence information: • Name information and person description • Associates • Hangouts • Vehicles • Employment history • Residence history • Telephone numbers • Suspicious activities • Other information investigators and other persons will want to record in the table		
The person's name, as with all names in the system, must be part of the central name table.		
System must limit access to intelligence information, allowing access to only those employees with appropriate security clearance, and preventing other users without appropriate security access from even knowing intelligence information exists for a specific person.		
System must provide an audit trail for input of data into the system.		
System must provide a mechanism to monitor the validation and verification of intelligence data.		
System must provide a mechanism for tracking intelligence information so that outdated and unverified information may be purged.		

Incident Based Reporting (IBR)

In addition to a general overview of Incident Based Reporting features, describe the ability of SYSTEM to meet the requirements listed in the table below.

Requirement	Response	Exceptions and Additional Costs
System must Provide for creation of IBR (Information Based Reporting) consistent with federal and state requirements.		
System must provide error checking and correction utilities that aid the user in reducing errors in IR submission to the state.		
Help screens must be available to the user to understand exactly how to correct errors and add missing information that is necessary in order to be compliant with state and national IBR requirements.		
The UCR program must automatically pull from information routinely entered through the application software and not require special data entry immediately prior to UCR generation.		
The program must create the following returns: • Monthly count of offenses known • Property by type and value • Property stolen by classification • Persons arrested 18 years and over • Persons arrested Under 18 years • Return of arson offenses • Law Enforcement officers killed/assaulted • Arrest and citation register • Domestic violence calls-assist • Violent crime to senior citizen		
System must allow for on-line submission as well as printing of the NIBRS reports.		

Crime Analysis

Requirement	Response	Exceptions and Additional Costs
System must provide investigators with the tools and information to analyze incidents and conduct thorough crime investigations including but not limited to: • Searches by MO • Searches by suspect physical description • Searches by weapon involvement • Searches by crime type by beat, zone, district, agency-wide • Searches by shift/date and time • Vehicle – suspect relationship searches • Scars, marks, tattoos • Any field in which data is entered • Matrix / relationship searches for persons, weapons, vehicles, telephone, addresses, etc.		
System must provide searching capabilities to allow users to access a host of information simply by searching on a given field and combine the data elements from multiple tables.		
System must enable users to attach and reference any number of reports or files associated with incidents or a person's name for fast access to related information.		
System must accommodate the use of automated pin mapping for crime analysis without use of third-party products.		
System must allow the map images to be translated into a format that can be exported to a file, printed, or otherwise saved. What formats are available?		
Maps must be able to be exported for use by other GIS software programs such as ESRI or MapInfo. What formats can be produced?		

Crime Interface

Requirement	Response	Exceptions and Additional Costs
The crime interface must transfer integrated information between the CAD system, law enforcement and Fire RMS.		
Allow the interface to copy information such as the record number and location of the incident into the crimes record after the user enters the command.		
System must have the ability to update limited CAD records from the field based on system securities.		
System must allow tracking of incidents between the CAD, Fire and Crimes modules.		

Patrol and Mobile Computing

Technical Requirements

Requirement	Response	Exceptions and Additional Costs
Does the system architecture support multi-tier deployment? Please describe proposed solution architecture.		
Does the system provide global search functions so that users can search system-wide based on name, address, vehicle information, property, etc. based on SOUNDEX, partial & wild-card search, AND "Google-like" search?		
Does the system provide multiple levels of data security control access including access by user and by group?		
Is system compliant with and/or capable of interface to FirstNet? Demonstrated capability is a requirement.		
All data must be backed up using 30-minute rolling backups to an offsite location. System performance must not be degraded during backups.		
Please provide a description of GIS integration.		
Mobile users can continue to work within the RMS.		

Requirement	Response	Exceptions and Additional Costs
The mobile system is designed for ease of use in the mobile environment.		
Font size is sufficiently large for mobile readability.		
Color-coding is used where appropriate to help convey key data at a glance.		
The mobile system can be easily switched between day and night mode display configurations with a single button, mouse click, or keystroke.		
System allows multiple forms of navigation including touch screen and mouse.		
Buttons are sufficiently large for touch screen access.		
The system shall provide the ability to roam in between multiple infrastructure formats – such as cellular and Wi-Fi.		
The system shall be capable of running sufficiently over slower wireless technologies such as RF data radios should the agency ever elect to do so. 9600 baud is the maximum speed requirement.		

Mobile General

Mobile Security and Accessibility

Requirement	Response	Exceptions and Additional Costs
Access to each component of the software can be granted or restricted for individual users or for groups of users.		
For each component, access levels include view, edit, print, delete, admin, etc.		
Access is verified by username and corresponding confidential password.		
Passwords are never displayed.		

Requirement	Response	Exceptions and Additional Costs
Each user has only one username and password for the entire system.		
CAD and RMS modules must be accessible with a single click or keystroke, without launching a separate program for each.		
The system tracks the individual who last entered or updated any transaction as well as the date of the modification.		
The system provides for multiple users, both mobile and non-mobile, to be using the same applications and accessing the same records simultaneously.		
Mobile workstations must be kept synchronized with agency servers so that CAD or RMS data entered on mobile units is immediately available on desktop workstations at the agency or vice versa, as long as the connection is established. If the connection is lost, any new data is automatically synchronized when the connection is re-established. In this way, the mobile system is completely integrated with the system's desktop CAD and RMS modules.		
The CAD system must seamlessly integrate with the RMS and be provided by the same vendor.		
The software provides a one-time, single-point of data entry that allows information to be accessible from other modules in order to provide the greatest operator and system efficiency.		
Hazards / alerts must be integrated between the CAD and RMS modules so that alerts entered in one area are available in the other.		
The CAD and RMS modules must share master databases for names, addresses, and vehicles so that records entered through CAD are added to these databases, and information from these databases added through the RMS are available in the CAD.		
The software provides the officer with access to RMS information on the reporter / complainant, incident address, and any involved vehicles. This data includes outstanding warrants, case involvements, etc.		
Officers must be able to quickly and easily perform an automatic transfer of information to the RMS when needed. This transfer must not be a one-time transfer but must be kept up to date as the CAD call progresses.		

Requirement	Response	Exceptions and Additional Costs
Call for service data must be readily available in the RMS to help officers in writing case reports. This information should include call for service type, location, complainant / reporters' names and addresses, narrative details, incident creation and clearance times, unit response times, etc.		
The software provides the ability to verify the quality of data entered into the database by performing immediate error checking, prohibiting invalid data from being saved.		
The software provides auto-completion capability for frequently entered information; once the user begins typing his/her selection, the appropriate data is automatically populated into the record.		
Users can use the Tab key to move quickly between fields.		
Required fields are easily identified by a visual indication (such as color-coded). If a user attempts to save a record without completing all required fields, the system will notify the user of the remaining required fields.		
Spell-checking is provided.		
Data entry and navigation are designed for the mobile environment. Where appropriate, functions can be performed with touch-screen buttons or mouse clicks, with minimal typing required.		

Data Entry Requirements

Mobile Configurability and Supervisor Functions

Requirement	Response	Exceptions and Additional Costs
The software's level of supervisor security is by user or user group.		
The software allows supervisors to maintain mobile users.		
The software allows supervisors to maintain mobile users' permissions.		
Where appropriate, fields and features can be turned on/off to best fit the agency's procedures.		

Requirement	Response	Exceptions and Additional Costs
The agency staff is able to adjust commonly altered variables such as codes, tables, report parameters, etc., without the services of a professional programmer or without contracting with the bidder.		
The software allows supervisors to maintain a list of mobile user locations so that mobile users do not have to manually type commonly used locations.		
The software allows supervisors to maintain a list of mobile user details so that mobile users do not have to manually type commonly used details.		
The software allows supervisors to configure default intervals for check-in reminders used to promote officer safety.		
The agency can configure how mobile users are alerted to events such as new incident assignments, new state / NCIC query returns, new instant messages, new email-style messages, and new bulletins. Options include visual and audible alerts as well as forcing the mobile CAD display to the front of any other programs the user has running.		
A supervisor can easily identify which officers are logged into the mobile system.		
A supervisor can easily monitor mobile users' dispatch activity from a remote location.		

Mobile CAD

Requirement	Response	Exceptions and Additional Costs
The mobile CAD system enables silent dispatch.		
The mobile CAD screen can be configured by the user in order to display the data most useful or relevant to the current situation.		
The mobile CAD system displays key data about on-duty units, including but not limited to call sign, status, location, key details (e.g. has ride-along), etc.		

Requirement	Response	Exceptions and Additional Costs
Mobile users can sort the Units display to show only a subset of units, such as units in a specified beat, available units only, assigned units only, etc.		
The software provides a means of indicating which units are using mobile CAD and are therefore available to receive communications through the mobile CAD system. This indication is available to both call takers / dispatchers and to other mobile users.		
The mobile CAD system displays key data about active incidents, including but not limited to incident number, priority, nature of call, address, and assigned units.		
Mobile users can choose to see all active incidents or only his/her own assigned incidents.		
Mobile users can quickly and easily view any and all incident information available to call takers / dispatchers that is not available on the main mobile CAD screen. This information includes but is not limited to: • Incident location • Nature of call • Priority • Beat • Complainant / reporter data and contact information • Narrative details • Any duplicate or linked incidents • Attached state / NCIC queries and returns		
Mobile users are able to update data about their assigned incidents entered by call takers / dispatchers. For example, update the street address if it was entered incorrectly or change the nature of the incident after arriving on scene. This data is made available for viewing by call takers / dispatchers and other mobile users.		
Mobile users can add unlimited narrative details to their assigned incidents. These details do not override any details entered by call takers / dispatchers and are available for viewing by call takers / dispatchers and other mobile users.		
This data is made available for viewing by call takers / dispatchers and other mobile users.		
A “use caution flag” can be placed on any incident by a call taker / dispatcher or officer and is made highly visible to all other users (dispatch or mobile).		

Requirement	Response	Exceptions and Additional Costs
Mobile users can create officer-initiated traffic stop incidents. This can be done with a single button, mouse click, or keystroke and does not require a separate action to assign self to the traffic stop.		
Upon creating a traffic stop incident, mobile users are presented with appropriate fields for entering traffic stop information such as location, vehicle data, driver data, etc.		
Mobile users can assign themselves to incidents with a single button, mouse click, or key stroke.		
Mobile users can self-status, i.e., independently perform any of the status options for their own unit that can be performed by call takers / dispatchers. Self-status can be done with a single button, mouse click, or key stroke. Status updates are immediately made visible to call takers / dispatchers and other mobile users with no radio communication required.		
Self-status actions include but are not limited to: • Mark self as on duty and available for dispatch • Assign self to an incident • Mark self as enroute or on scene at an incident • Mark self as leaving scene or having completed an incident • Mark self as busy / unavailable for dispatch • Mark self as off-duty or on call		
Mobile users can easily update their own locations. Common locations (such as North Station, South Station, Jail, Hospital, etc.) can be selected with a button or mouse click instead of requiring the mobile user to type. Location updates are immediately made visible to call takers / dispatchers and other mobile users with no radio communication required.		
Mobile users can easily update their own key details. Common key details (such as Has Ride-along, Has Prisoner, On Foot, etc.) can be selected with a button or mouse click instead of requiring the mobile user to type. Details updates are immediately made visible to call takers / dispatchers and other mobile users with no radio communication required.		
Call takers / dispatchers can continue to update statuses, locations, details, etc. for mobile users should an officer lose connection, step out of his/her vehicle, etc.		
Mobile users are visually alerted when the agency-defined check-in time for officer safety has passed. The mobile user can "check in" with a single button, mouse click, or keystroke with no radio communication required.		

Requirement	Response	Exceptions and Additional Costs
Mobile users are visually alerted when an incident's agency-defined dispatch timer (based on nature of incident and priority) has passed without any units having been assigned.		
A mobile user who is assigned to a call can easily "stack" him/herself on a second call, providing a visual indication to call takers / dispatchers and other mobile users that he/she will respond to the call after handling the current call. Stacking is unlimited.		
A mobile user who is assigned to a call can reassign him/herself to a higher priority call and "stack" him/herself to the initial call.		
All name, address, and vehicle alerts such as outstanding warrants, officer safety threats, medical alerts, hazardous materials alerts, protection system or water supply information, and other agency-defined alert types are highly visible to mobile users.		
From the mobile CAD system, users can easily access all previous involvements about individuals, businesses, addresses, and vehicles such as prior calls for service, traffic stops, case involvements, summons / citations / tickets, jail stays, warrants, parking tickets, etc.		

Mobile RMS General

Requirement	Response	Exceptions and Additional Costs
The mobile RMS system provides mobile users permission-based access to the RMS features and functions available from desktop workstations, with similar navigation and displays so that officers can use mobile units OR desktop workstations without having to learn new procedures.		
The software uses a synchronizing method to keep case reports and other RMS records up-to-date between the agency and mobile users.		

Requirement	Response	Exceptions and Additional Costs
Mobile users can continue to work within the RMS system (typing case reports, etc.) even when the connection is lost. Any new data is automatically synchronized when the connection is re-established.		
Use of mobile RMS functions does not prevent mobile users from being immediately alerted to dispatch information such as new incident assignments, instant messages, bulletins / BOLOs, etc.		

Mobile RMS: Name, Address and Vehicle Records

Requirement	Response	Exceptions and Additional Costs
Mobile users can view and update all recorded data about a person, including but not limited to: • Name (first, middle, last, suffix) • Sex • DOB / Age • Address (street, city, state, zip code) with history • Telephone numbers (unlimited) • Aliases • Occupation • Ethnicity / Race • Physical description • Scars / Marks / Tattoos • ID numbers (including but not limited to driver's license number, social security number, state ID number, FBI number, arrest number, fingerprint classification number, etc.) • Additional agency-defined ID numbers • Education • Marital status • Religion • Citizenship • Place of birth • Unlimited mugshots • Relationship data (next of kin, known associates, employers, etc.)		

Requirement	Response	Exceptions and Additional Costs
Mobile users can access a listing of all activity a person / business was involved in, including calls for service, case reports, jail bookings, summons/citations/tickets, parking tickets, warrants, registered vehicles, etc.		
Mobile users can follow a link to any records in which the person was involved.		
Names are automatically added to the master name database when entered on a record by a mobile user, or mobile users can manually add new names.		
The software has built-in checking to reduce the possibility of creating duplicate master name records for the same individual.		
The software automatically checks a name against the list of outstanding warrants and notifies the mobile user.		
The software automatically checks a name against the list of known sex offenders and notifies the mobile user.		
The software automatically checks a name against the list of current jail inmates and notifies the mobile user.		
The system automatically displays any user-entered name alerts (medical alerts, officer safety threats, and other agency-defined alert types).		
Mobile users can easily create new name alerts from a master name record.		
Mobile users can access and search the master address database.		
Mobile users can access a listing of all activity an address was involved in, including calls for service, case reports, etc., and link to those records if their permission level allows.		
The system automatically displays any user-entered address alerts to mobile users (hazardous materials, alarm system, water supply information, officer safety threats, and other agency-defined alert types).		
Mobile users can easily create new address alerts from a master address record.		
Mobile users can access and search the master vehicle database.		

Requirement	Response	Exceptions and Additional Costs
Mobile users can view and update all recorded data about a vehicle, including but not limited to: • License plate number • Plate expiration • Plate state • Plate type • Vehicle year • Make • Model • Color • Secondary color • Style • VIN • Features • Registered owners (with history)		
Mobile users can access a listing of all activity the vehicle was involved in, including calls for service, traffic stops, tow calls, case reports, summons/citations/tickets, field identifications, parking tickets, etc., and link to those records if their permission level allows.		
The system automatically displays any user-entered vehicle alerts to mobile users (including agency-defined alert types).		
Mobile users can easily create new vehicle alerts from a master vehicle record.		

Mobile Case Reporting

Requirement	Response	Exceptions and Additional Costs
Mobile users can generate a case report from a CAD call at any time. This transfer must not be a one-time transfer but must be kept up to date as the CAD call progresses.		
Case reports generated from calls are auto-populated with data such as address, nature of the incident, complainant / reporter data, etc.		

Requirement	Response	Exceptions and Additional Costs
When case reports are generated from calls for service, incident data such as responding units and unit response times is readily available to assist in completing the case report.		
Case reports can be generated without corresponding calls for service.		
Mobile users can enter and update case report data, including but not limited to: • Date / time • Primary officer • Case disposition • Nature of incident • Location • Assisting officers • Unlimited narrative text, both primary and supplemental • Offenses • Names / involved parties • Search warrants		
Mobile users can attach documents and files (Word, Excel, etc.) to case narratives.		
Mobile users can access and search the list of all of the agency's case reports, whether they were created at the agency or by any mobile user.		
The case report list can be filtered or queried by data elements such as date, case report type, status, primary officer, disposition, nature of incident, names of involved parties, offenses, case number, etc.		
The system includes a "Google-like" searching capability for all narrative elements of case reports.		

Mobile Case Management

Requirement	Response	Exceptions and Additional Costs
The mobile RMS integrates seamlessly with the software's case management system so that the entire case creation, approval, and referral process can be performed by officers and supervisors working from mobile units in the field.		
All case management features and functions are accessible by mobile users, including but not limited to: • Mobile users can create and update case reports • Mobile users can indicate that they have finished work on a case report and it is awaiting approval • Mobile users with appropriate permission (supervisors) can "kick back" cases with comments indicating needed changes • Mobile users with appropriate permission (supervisors) can approve cases and thereby lock them against future editing • Mobile users with appropriate permission can reactivate cases • Mobile users have quick access to a list of cases for which they have unfinished tasks (complete case, add to case, approve case, review case, etc.) • Mobile users can complete referral forms for case reports; based on user input, notification and follow up tasks can be generated • Mobile users can receive alerts such as when a case report has aged beyond an agency-defined number of days • Mobile users can send and receive email-style messages containing links to case reports • Mobile users can query the case list to view an officer's case load, generate a case summary for a time period, etc. • Mobile users can access a list of calls for service requiring case reports that have not yet been written		
Mobile users with appropriate permission can add or update property / evidence items.		
Digital photos can be uploaded to case reports from mobile units.		
Digital audio files (such as interviews) can be uploaded to case reports from mobile units.		
Mobile users can view digital photos added on desktop workstations or by other mobile users.		
Mobile users can listen to audio files added on desktop workstations or by other mobile users.		

Mobile Property and Evidence

Requirement	Response	Exceptions and Additional Costs
Mobile users can enter and update arrest information including but not limited to: • Date of Arrest • Time of Arrest • Location of Arrest • Arrest Type (on-view, etc.) • Name of Arrested Person • Arresting / Assisting Officers • Charges • Court Date / Time • Comments (unlimited)		
Arrest forms entered from mobile units are made available in the jail module and can be auto populated into a booking record.		

Mobile Summons / Citations / Tickets

Requirement	Response	Exceptions and Additional Costs
Mobile users can enter and update summons / citations / tickets, with data including but not limited to: • Ticket type (citation / warning, traffic / other) • Officer • Court and disposition data • Ticket number • Date / time issued • Offender name, address, and ID numbers • Location • Offenses • Vehicle information (plate number and state, year, make, model, color, style, VIN, registered owners, etc.) • Speed clocked, speed cited, speed limit • Narrative details and comments • Associated case report number		
Mobile users can access a list of summons / citations / tickets and query it by data elements such as date range, offender name, ticket number, driver's license number, license plate number, etc.		

Requirement	Response	Exceptions and Additional Costs
Mobile users can enter and update field identification forms to record information about people and vehicles identified, with data including but not limited to: • Officer • Date and time • Identification method • Location • Name of person identified, address, DOB, SSN, etc. • Person's dress, such as gang colors • Pertinent vehicle information (plate number and state, year, make, model, color, style, VIN, registered owners, etc.)		
Mobile users can access a list of field identification forms and query it by data elements such as date range, officer, individual's name, driver's license number, license plate number, etc.		

Mobile Warrant File Functions

Requirement	Response	Exceptions and Additional Costs
Mobile users can access a warrant log that can be queried / filtered by data elements including: • Date issued • Date served • Date recalled • Warrant type • Status • Name • Address • File transaction number • Court warrant number		
Mobile users with adequate permission can record that a warrant has been served.		
Mobile users are alerted to names with active warrants while using any screen or feature of the mobile system.		

Resource Management

Requirement	Response	Exceptions and Additional Costs
Tracking availability and location of resources such as forklift, backhoe, jaws of life, etc.		
Record of contact person or business for obtaining equipment and other resources		
Comments section for notes/pertinent information and rates.		

CAD Mapping and Automatic Vehicle Location (AVL) Mapping

In addition to a general overview of the CAD Mapping and Automatic Vehicle Location (AVL) mapping capabilities, describe the ability of SYSTEM to meet the requirements listed in the table below.

Requirement	Response	Exceptions and Additional Costs
System must have the capability to integrate AVL with the CAD system.		
System must have the capability to phase in AVL after the base system has been implemented. Allow for various layers for individual agency departments' use controlled by system securities.		
The CAD module must display the two cross streets nearest a given address and any special directions entered.		
The CAD module must enable the user to add an alert(s) to the address and display the alert(s) if the address is entered previously anywhere in the system.		
The CAD module must enable the user to define apartment/ office buildings thus enabling the software to identify specific apartments in the Geographic Database.		
The CAD module must track the location of all fleet units through Global Positioning System (GPS) receivers.		
The CAD module must locate the coordinates of all units on a map allowing dispatchers to quickly assign units to calls closest to the unit's current location.		

Requirement	Response	Exceptions and Additional Costs
The CAD module must display locations of current CAD calls, as calls are added, modified, or completed allowing dispatchers to view calls and units in a geographical environment.		
The CAD module must allow officer locations and call location information to be plotted automatically onto a map.		
The CAD module must display locations of current CAD calls, as calls are added, modified, or completed allowing dispatchers to view calls and units in a geographical environment.		
The CAD module must allow officer locations and call location information to be plotted automatically onto a map.		
The CAD module should use drag and drop functionality on the map in order to dispatch units to a call.		
The CAD module must allow agencies to create multiple map layers in ESRI, import them to a map and change the order of the layers to enhance visibility. The CAD module must control zoom, pan, and display functions directly from the CAD command line. System must have computerized mapping of crime and call data to include the ability to "fence" particular areas as desired.		
The AVL module must have the ability to record, archive and replay vehicular movement and speed.		

NG9-1-1 Interface

In addition to a general overview of the NG9-1-1 Interface, describe the ability of SYSTEM to meet the requirements listed in the table below.

Requirement	Response	Exceptions and Additional Costs
The system must provide an integrated interface between the CAD system and NG9-1-1 system.		
When a Request for Emergency Assistance comes in, the system must allow for downloading the contact phone, address, and agency from the NG9-1-1 system into the call entry record without additional data entry using ANI/ALI		

Requirement	Response	Exceptions and Additional Costs
The NG9-1-1 interface must be able to receive location data (cell sector and x, y, z coordinates) from wireless devices and wireless service providers.		
The NG9-1-1 interface must be able to store the raw call information in the call record.		
The NG9-1-1 interface must be able to log calls for troubleshooting.		
The NG9-1-1 interface must be able to run in a debug mode for raw data troubleshooting.		
The NG9-1-1 interface must be E9-1-1 Phase II compliant at a minimum and should be configured to support additional location information as that information is made available, without additional cost to the ECC.		
The NG9-1-1 interface, and CAD system overall, must be capable of sharing data with other ECC's, without the need for proprietary interfaces at additional cost to the ECC.		

Geographic Database

In addition to a general overview of the Geographic Database – Address Verification capabilities, describe the ability of SYSTEM to use a common address file for all modules reducing the chance of misspelled names or erroneous block numbers being entered into the system. Incidents based on addresses can be related with less chance of oversight or error.

Describe how SYSTEM can meet the following specific requirements.

Requirement	Response	Exceptions and Additional Costs
System must utilize Soundex or more advanced search methods for finding/verifying sound alike or misspelled addresses.		
System must verify addresses, number ranges, street names, intersections, street aliases, mileposts, rural routes, and commonplace names.		
System must accommodate the use of mile markers, highway exits, and street intersections and overpasses.		

Requirement	Response	Exceptions and Additional Costs
System should allow for entry of a non-Geographic Database address and request an address update to Geographic Database at a later time. Must provide a report of all invalid addresses.		
System must utilize a common address file to ensure that street names are valid and spelled correctly.		
System must utilize a common address file to ensure that street address block numbers are valid.		

CAD Interface to Fire/EMS Records Management

Requirement	Response	Exceptions and Additional Costs
The system vendor must be willing to collaborate with the Fire/EMS Services RMS vendor to establish an interface between the two application systems in order to meet the following requirements. The Fire/EMS Services RFP will contain similar language requiring this collaboration effort.		
It is preferred that system CAD module create Fire Records Management System records from CAD calls. Describe the ability of your system to interface with a Fire records management system licensed by another vendor.		
Provide the ability to allow alerts to be sent to the EMS/FIRE personnel who are treating an individual who may be wanted or have a warrant.		
It is preferred that system CAD module can create EMS Records Management System records from CAD calls. Describe the ability of your system to interface with an EMS Records Management System licensed by another vendor.		
The system CAD module must provide any required unit times for Fire/EMS dispatches, including: • time the call is dispatched, • time the assigned unit responded, • time the unit is on scene, • time the unit is back in service, and • time the unit arrives back in the station.		

System Acceptance Testing / Compliance Matrix

System Acceptance Testing

Equate each major requirement above to a specific performance metric here:

- Comply
- Does Not Comply
- Comply with Exception (with description)

Acceptance Testing and Failures Identification

Acceptance Testing

1. Agency will create a written acceptance plan created after award of the contract based on the equipment selected. Agency will not accept or certify the equipment until all items on the acceptance test plan are met to the satisfaction of the agency.
2. The Bidder will be responsible for all materials, hardware, and software provided until subject items have been delivered, implemented, tested, and accepted by agency.
3. The vendor will certify in writing to agency when the system is installed and ready for testing. Degrees of system failure and operability for acceptance testing purposes are determined solely by agency.

Failure Levels

The following failure priority levels are defined for use during the Systems & Acceptance Testing process:

a. Major failures are major system failures that render the system completely unusable or significantly reduce system operability and are considered to be operationally unacceptable by agency.
b. Minor failures are minor system failures or open punch list items that minimally reduce system operability or have little or no effect on system operability and usability and are considered to be operationally acceptable only during the acceptance testing phase by agency.

Final Acceptance Testing

1. Final acceptance testing is expected to commence immediately upon system cut over and proceed for fourteen (14) consecutive major alarm failure free days. If a Major failure occurs during the final acceptance testing period, the final acceptance testing period will be stopped, and the failure or failures expediently fixed to Agency's satisfaction. Response times to failures must meet the requirements defined for the warranty period.

2. During this period of interruption, the system must continue to operate with the greatest degree of reliability possible given the respective failure(s). The final acceptance testing period of fourteen (14) consecutive failure free days will restart the day after repairs are affected, at agency's sole discretion.

3. **Measurable Testing**
Testing must include a measurable testing process for each functional and technical aspect of the specifications listed in the Bidder's proposal, and system performance measurements based on the telephone activity to date in Agency's ECCs. This testing serves as a sign off process for payment to the vendor.

4. **System Failures Due to External Causes**
In measuring acceptance, system failures resulting from external causes, including but not limited to acts of God, fire, or agency supplied hardware, software, or connectivity failure, will be excluded from the acceptance testing.

Equal Opportunity
(Placeholder for agency specific requirements)

Insurance Requirements
(Placeholder for agency specific requirements)

General Terms and Conditions
(Placeholder for agency specific requirements)

Finances
(Payment Terms and Conditions)
(Placeholder for agency specific requirements)

Signatures
(Placeholder for Signature page specific to agency).

Addendum 1 – Terms and Conditions

(Contents of vendors proposal may become contractual obligation, etc.)

Addendum 2 – Respondent's Warranty

System warranty and system maintenance periods for all hardware, software, and on-site maintenance shall begin upon final acceptance of the entire system and shall run concurrently for a period of 12 months. Pricing for system warranty and system maintenance for the initial 12 month period shall be included in the base price. If there are multiple maintenance support level options, please price them separately.

Bidder shall guarantee the availability of service assistance, repairs, and spare parts for a minimum of seven (7) years after equipment delivery.

A complete listing of all warranties including systems and equipment, detailing what is included and what is not included shall be included.

24 hour technical and maintenance support must be available with a response time, on-site, of no more than four (4) hours for major failures. This should be available 24x7x365.

Addendum 3 – Governance

The agency should detail their specific governance structure in this section. Governance is critical to the success of any NG9-1-1 program and making the vendors fully aware of how the system will be managed is an important part of the process. More important is the need to get all parties who will use and maintain the system to agree on how that will be accomplished.

The governance planning process is the step 9-1-1 Authorities should consider taking to develop how the NG9-1-1 system will be managed and used to guide its future activities. Governance models developed may include:

- Identifying the group that will have the authority, knowledge, and commitment to make decisions about the migration to NG9-1-1.
- The body that will oversee the NG9-1-1 system when it is in production.
- The method of interaction between the project team and governing body, including project team authority levels for changes and identification of the change process.

Handouts

There are several one-page handouts included in this guide. Keeping the audience in mind, this tool may provide an overview of the information on a single page. Additionally, this can be used as read-ahead information to introduce NG9-1-1 to the reader and prepare them for a further conversation. Each has a particular perspective summarizing essential points in a customizable one-page layout that may assist in capturing the reader's full attention in an easy-to-read format.

APCO International
Leaders in Public Safety Communications®

Next Generation 9-1-1 for the ECC Director

CHALLENGES FOR NG9-1-1

- NG9-1-1 has the promise to match the experience and expectations of the public directly with the ECC.
- NG9-1-1 capabilities include voice, text, video, picture, and other call-related data.
- Use of the APCO RFP template can lead to a better integrated, efficient, and cost-effective procurement to begin to match the public's capabilities.
- Developing strategies to address the impacts of NG9-1-1 on the ECC workforce will be critical.

ECCs will have the ability to receive new forms of data from the public, possess the tools needed to process, triage, and analyze this information, and be able to share incident data in a fully interoperable manner with other ECCs and field-based responders.

Citizens requesting emergency assistance will receive a similar experience no matter what ECC receives the emergency request for service without delay and without the need for additional applications, services, or actions by the public safety telecommunicators (PST) to access critical information.

There are opportunities for 9-1-1 authorities and ECCs to move beyond the status quo of limited, staged deployments that lack interoperability. What is needed is the right incentives to influence the NG9-1-1 vendor community to deliver on public safety's requirements. These include a request for proposals (RFP) process that pursues complete, end-to-end solutions and is objectives-based, such as to require interoperability, security measures, and other key requirements

The human element remains most important regardless of innovations in technology. The operational impacts of NG9-1-1 implementation will drive new training and workforce requirements. The stress levels, work environments, expectations, and job conditions can overwhelm veteran and newer staff members. With the increased broadband capabilities, ECCs will be expected to do more with the same staffing. In some instances, ECCs may need to hire additional staff with enhanced skillsets but remain within a limited staffing and training budget. ECC policies must account for new skillsets, potential new positions, cyber and physical security, and ECC personnel's mental health and wellbeing.

APCO International
Leaders in Public Safety Communications®

Next Generation 9-1-1 for the Chief or Sheriff

BENEFITS OF NG9-1-1

- NG9-1-1 provides the ECC the same communications capabilities available to the public.
- The increased amount of data and video analytics products and social media mining and aggregation tools, will provide new opportunities for real-time analysis of active incidents.
- This will lead to enhanced situational awareness for 9-1-1 professionals and emergency responders.
- Sustainable funding for NG9-1-1 necessitates planning for lifecycle replacement.

Next Generation 9-1-1 (NG9-1-1) promises to match the experience and expectations of the public that use connected devices (including smartphones, tablets, and gaming platforms), and share all types of data, including their location, text, photos, videos, and social media posts with each other, directly with the emergency communications center (ECC).

However, public safety must think of NG9-1-1 in a comprehensive, end-to-end fashion. Essentially, NG9-1-1 needs to mean the ability of ECCs to receive new forms of data from the public, possess the tools necessary to process, triage, and analyze this information, and share incident data in a fully interoperable manner with other ECCs and responders in the field. Described this way, NG9-1-1 does not yet exist anywhere in the country.

Interoperability is the capability of ECCs to receive 9-1-1 requests for emergency assistance, then process and share this information with other ECCs and emergency response providers without the need for proprietary interfaces and regardless of jurisdiction, equipment, device, software, service provider, or other relevant factors.

Ensuring adequate funding for NG9-1-1 is one of the most significant challenges faced and preparing and implementing NG9-1-1 is only the first step in the technology ecosystem lifecycle process. It is necessary to plan for the continual refresh of hardware, software, and user equipment throughout the system's technical maturity.

APCO International
Leaders in Public Safety Communications®

Next Generation 9-1-1 for the Public Safety Telecommunicator

BENEFITS OF NG9-1-1

- NG9-1-1 provides the ECC the same communications capabilities available to the public.
- The increased amount of data and analytical analysis will enhance situational awareness for 9-1-1 professionals and emergency responders.
- Cybersecurity training will be ongoing to address emerging threats to ECC.
- The operational impacts of NG9-1-1 implementation will drive new training and workforce requirements.

Next Generation 9-1-1 (NG9-1-1) has the promise to match the experience and the expectations of the public directly with the public safety telecommunicator (PST).

PSTs will have the ability to receive new forms of data from the public and will possess the tools needed to process, triage, and analyze this information, and be able to share incident data in a fully interoperable manner with other ECCs and responders in the field. NG9-1-1 will increase the visibility and significance of the PST in the call taking process.

Persons requesting emergency assistance will receive a similar experience no matter what communications center the PST is located at without delay and without the need for additional applications, services, or actions by PST to access critical information.

PSTs will require additional training in cybersecurity, data analysis, and criteria-based call taking that standardizes the aspect of call taking and extends to the sharing of actionable data between ECC in a consistent and interoperable manner.

PSTs will still need important skills such as enhanced multitasking, critical thinking, strategic decision making, problem identification, and analytical analysis. PSTs will expand on existing knowledge, skills, and abilities, including cybersecurity awareness, familiarity with digital, broadband, and IP-based technology, and the ability to sift through and prioritize increased volumes and data types.

APCO International
Leaders in Public Safety Communications®

Cybersecurity for Next Generation 9-1-1

CHALLENGES FOR NG9-1-1

- ECCs are high-level and high-visibility targets to cyber criminals.
- IP-based networks provides new access into the ECC.
- ECC vendors must build in cybersecurity within the system design- "baked in".
- Security patches and system updates can reduce exposure to cyberattack.
- ECCs should adopt an in-service training program that serves the needs of the ECC and its members. APCO recommends members receive four to eight hours of cybersecurity training annually.

ECCs are a high-level target for cyber criminals and NG9-1-1 will present new and different challenges and threats to disrupt emergency communications systems and ECC capabilities. This means cybersecurity protections should be incorporated by design into planning, implementation, and operation models from the onset. Viewing cybersecurity in this manner will reduce the need for costly, after-the-fact solutions that may not meet the level of security protections required by emergency communications.

As ECCs transition to IP-based technologies, 9-1-1 systems will transition from operating on networks with limited access to sharing networks with other ECCs, agencies, and vendors. This open environment will create new ways to access emergency communications networks. With these new capabilities, an increased risk of a cyberattack is likely if cybersecurity measures are not implemented into the system. ECCs should work with their vendors to ensure that systems are appropriately patched and determine schedules, processes and procedures for security updates.

ECCs will need to ensure that their technical and operational cybersecurity protocols are sufficient for both an NG9-1-1 and a legacy environment. ECCs must also create policies and procedures to help guide employees toward a secure NG9-1-1 ecosystem. When creating these policies and procedures, it is essential to gather the perspective of jurisdictional stakeholders, including IT staff, ECC leadership, and any local personnel that maintain systems and networks.

ECCs should adopt an in-service training program that serves the needs of the ECC and its members. APCO recommends members receive four to eight hours of cybersecurity training annually.

APCO International
Leaders in Public Safety Communications®

Next Generation 9-1-1 for Elected Officials

BENEFITS OF NG9-1-1

- 9-1-1 is more than 50 years old.
- The technology used in 1968 is still being used today.
- 9-1-1 capabilities do not match those of the public
- NG9-1-1 can change that, and support voice, text, video, pictures, and other important information provided by the public.
- NG9-1-1 does not solve location accuracy issues and still relies on the service provider/carrier.
- Federal support is needed for the nationwide transition to NG9-1-1. Public Safety organizations believe the costs may be greater than $15 billion dollars to fully fund NG9-1-1.

Public safety telecommunicators (PSTs) have been providing highly skilled and professional services to 9-1-1 callers for more than 50 years. Congress first adopted 9-1-1 as the national emergency number in 1968 to leverage the technology of that era to provide the public with a streamlined way to call for help.

Today, Next Generation 9-1-1 (NG9-1-1) promises to match the experience and expectations of the public that use connected devices (including smartphones, tablets, and gaming platforms), and share all types of data, including their location, text, photos, videos, and social media posts with each other. Regardless of the service provider, device, and manufacturer, the public can communicate and exchange information directly and without delay through various applications and services.

A common misperception is that NG9-1-1 will improve location accuracy or routing. That is incorrect. Wireless carriers are, and should be, responsible for determining the caller's location and routing the call to the appropriate emergency communications center. What is true is that GIS, in an NG9-1-1 environment, will enable much greater visual clarity into these functions.

No federal laws or regulations govern NG9-1-1, but several existing laws and regulations have implications for, and will likely extend into, an NG9-1-1 environment. Federal and state governance bodies should adopt modern definitions of key terms like NG9-1-1 and interoperability. States should address outdated laws and regulations that will inhibit the transition to NG9-1-1. All levels of government should avoid legislative, regulatory, and procurement approaches that shift responsibility from service providers to public safety. Federal support is needed for the nationwide transition to NG9-1-1, but we should preserve state and local control of 9-1-1.

APCO International
Leaders in Public Safety Communications®

Next Generation 9-1-1 for the Public

BENEFITS OF NG9-1-1

- 9-1-1 is more than 50 years old.
- Advanced capabilities the public uses do not match those of the ECC.
- NG9-1-1 can change that, and support voice, text, video, pictures, and other important information provided by the public directly to those who can help.
- NG9-1-1 does not solve location accuracy issues and still relies on the service provider/carrier of the person requesting emergency assistance.
- Being able to communicate directly with PSTs improves the police, fire, and EMS response.

Public safety telecommunicators (PSTs) have been providing highly skilled and professional services to 9-1-1 callers for more than 50 years. Congress first adopted 9-1-1 as the national emergency number in 1968 to leverage the technology of that era to provide the public with a streamlined way to call for help.

Today, Next Generation 9-1-1 (NG9-1-1) promises to match the experience and expectations of the public that use connected devices (including smartphones, tablets, and gaming platforms), and share all types of data, including their location, text, photos, videos, and social media posts with each other. Regardless of the service provider, device, and manufacturer, the public can communicate and exchange information directly and without delay through various applications and services.

The public should rightly expect any emergency communications center (ECC) to do the same without delay. The public relies on PSTs to accurately determine what resources are required for any situation and share any necessary data and information with police, fire, and EMS responder agencies throughout the incident.

A common misperception is that NG9-1-1 will improve location accuracy or routing. That is incorrect. Wireless carriers are, and should be, responsible for determining the caller's location and routing the call to the appropriate ECC. The public must still be prepared to provide location and scene safety information when calling 9-1-1.

Acronyms List and Definitions

3GPP
Third Generation Partnership Project. Unites seven telecommunications standard development organizations, known as "Organizational Partners" and provides their members with a stable environment to produce the Reports and Specifications that define 3GPP technologies.

9-1-1 Request for Emergency Assistance
A communication, such as voice, text, picture, multimedia, or any other type of data that is sent to an ECC for the purpose of requesting emergency assistance.

AAR
After Action Report. A structured review or debriefing after the fact to determine what happened, why it happened, and how it can be done better.

ACD
Automatic Call Distribution. It is a telephony system that automatically receives incoming calls and distributes them to an available PST.

ADA
Americans with Disabilities Act. The ADA is a civil rights law that prohibits discrimination against individuals with disabilities in all areas of public life, including jobs, schools, transportation, and all public and private places that are open to the public. The purpose of the law is to make sure that people with disabilities have the same rights and opportunities as everyone else. The law was interpreted to require that local governments ensure that their telephone emergency number systems are equipped with technology that will give hearing impaired and speech impaired individuals a direct line to emergency services.

AI
Artificial Intelligence. The term 'artificial intelligence' means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments.

ALI
Automatic Location Identification. The automatic display at the ECC 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. Working with Automatic Number Identification, the use of a database to associate a physical location with a telephone number. ALI is a feature of Enhanced 9-1-1 (E9-1-1) systems. ALI is provided to agents answering E9-1-1 calls. It may include information such as name, phone number, address, nearest cross street, and special pre-existing conditions. On some systems, it may also provide the appropriate emergency service address for the particular address. ALI is retrieved from a computer database that may be held on site or at a remote location.

ANI
Automatic Numbering Identification. Telephone number associated with the access line from which a call originates. The calling party's telephone number which is transmitted through the network on an out-of-band channel.

ANS
American National Standard. A document that has been sponsored by an American National Standards Institute (ANSI)-Accredited Standards Developer, achieved consensus, met ANSI's Essential Requirements, and been approved by the ANSI.

ANSI
American National Standards Institute. The American National Standards Institute is a private, not-for-profit organization that oversees the creation, promulgation and use of thousands of norms and guidelines that directly impact businesses in nearly every sector. ANSI facilitates the development of American National Standards by accrediting the procedures of standards developing organizations (SDOs). These groups work cooperatively to develop voluntary national consensus standards.

APCO
The Association of Public-Safety Communications Officials. APCO International is the world's oldest and largest organization of public safety communications professionals and supports the largest U.S. membership base of any public safety association. It serves the needs of public safety communications practitioners worldwide – and the welfare of the general public as a whole – by providing complete expertise, professional development, technical assistance, advocacy and outreach.

APCO ASAP
Automated Secure Alarm Protocol. A national service that is the next generation for the processing of information from alarm monitoring stations needing emergency dispatch. This protocol was founded through the partnership of APCO, Central Station Alarm Association (CSAA) and National Law Enforcement Telecommunications System (NLETS) – receiving government recognition and funding since 2010.

Apps
Applications. A software program that provides functionality in some area of human or business interest. There are apps for smartphones, tablet computers, personal computers, etc.

ASD
Accredited Standards Developer. An organization that voluntarily submits documentation of its procedures to ANSI for review and agrees to maintain compliance with ANSI's requirements and oversight.

ATIS
Alliance for Telecommunications Industry Solutions. ATIS is accredited by the ANSI. The organization is the North American Organizational Partner for the 3GPP, a founding Partner of the one M2M global initiative, a member of the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL).

AVL
Automatic Vehicle Location. A system for automatically determining and transmitting the geographic location of a vehicle.

BYOD
Bring Your Own Device. When an employee uses their own personal devices to connect to the agency's network and access what they need to do their jobs.

CAD
Computer Aided Dispatch. A computer-based system, which aids PSTs by automating selected dispatching and record keeping activities. The use of a computer-based system by a PST to electronically transmit incident details to computers in emergency vehicles.

CAMA
Centralized Automatic Message Accounting. An analog trunk originally developed for long-distance billing and used for emergency 9-1-1/E9-1-1 services.

CFS
Call For Service. An emergency or non-emergency request for service that generates a record within CAD and RMS systems.

CISA
Cybersecurity & Infrastructure Security Agency. An agency within the Department of Homeland Security that leads the national effort to understand, manage, and reduce risk to cyber and physical infrastructure.

CISM
Critical Incident Stress Management. An adaptive, short-term psychological helping-process that focuses solely on an immediate and identifiable problem. It can include anything from pre-incident preparedness to acute crisis management to post-crisis follow-up.

CJIS
Criminal Justice Information Services. The CJIS Division was established in February 1992 out of the former Identification Division to serve as the focal point and central repository for criminal justice information services in the Federal Bureau of Investigations (FBI).

Commonly Accepted Standards
The term 'commonly accepted standards' means the technical standards followed by the communications industry for network, device, and IP connectivity that (a) enable interoperability, and (b) are (i) developed and approved by a standards development organization that is accredited by an American or international standards body (such as ANSI) in a process that is open to the public, including open for participation by any person and provides for a conflict resolution process; (ii) subject to an open comment and input process before being finalized by the standards development organization; (iii) consensus-based; and (iv) made publicly available once approved."

CPE
Customer Premise Equipment. Terminal equipment (telephones, key systems, Private Branch Exchanges (PBXs), modems, video conferencing devices, etc.) connected to the telephone network and residing on the customer's premises.

CSRIC
FCC Communications Security, Reliability, and Interoperability Council to provide recommendations to the FCC for a range of public safety and homeland security-related communications matters.

CVVA
Twenty-First Century Communications and Video Accessibility Act. The CVAA amended the Communications Act and imposed a variety of new obligations on service providers, equipment manufacturers, and the Commission that relate to providing access to communications services for people with disabilities.

COMSTAT
Computer Statistic. Accurate and timely intelligence related to the statistical analysis of data.

COTS
Commercial Off The Shelf. Products including hardware and software that are adapted to aftermarket needs and designed to be easily installed and to interoperate with existing technologies.

DHS
Department of Homeland Security. A federal agency designed to protect the United States against threats. Its wide-ranging duties include aviation security, border control, emergency response and cybersecurity.

DMZ
Demilitarized Zone. In computer networks this is a physical or logical subnet that separates a LAN from other untrusted networks.

E9-1-1
Enhanced 9-1-1. 1. Landline Enhanced 9-1-1: the telephone number of the caller is transmitted to the ECC, where it is cross-referenced with an address database to determine the caller's location. That information is then displayed for the emergency dispatcher to direct public safety personnel responding to emergencies. 2. Cell phone Enhanced 9-1-1: Phase II E9-1-1. The FCC requirement that wireless carriers provide the location – within approximately 165 to 330 feet of anyone dialing 9-1-1 from a cell phone.

EC3
Emergency Communications Cybersecurity Center. In the proposed NG9-1-1 cybersecurity architecture, the EC3 will take on the role of providing Intrusion Detection and Protection (IDPS) to ECCs and any other emergency communications services that would benefit from utilizing centralized, core cybersecurity services.

ECC
Emergency Communications Center. The term 'emergency communications center' means (a) a facility that (i) is designated to receive a 9-1-1 request for emergency assistance; and (ii) performs one or more of the following functions: process and analyze 9-1-1 requests for emergency assistance and information and data related to such requests; dispatch appropriate emergency response providers; transfer or exchange 9-1-1 requests for emergency assistance and information and data related to such requests with other ECCs and responders in the field; analyze any communications received from emergency response providers; and support incident command functions.

EIDD
Emergency Incident Data Document. The Emergency Incident Data Document (EIDD) provides a standardized, industry-neutral National Information Exchange Model (NIEM) conformant (XML-based) specifications for exchanging emergency incident information to agencies and regions that implement NG9-1-1 and IP-based emergency communications systems. Emergency incident information exchanges supported by the EIDD include exchanges between disparate manufacturers' systems located within one or more public safety agencies and with other incident stakeholders.

EIDO
Emergency Incident Data Object. Uses JavaScript Object Notation (JSON) format to share information. EIDO also incorporates elements from the NIEM.

EMD
Emergency Medical Dispatch. A systematic program of handling medical calls. Trained PSTs, using locally approved criteria-based guide cards, quickly and properly determine the nature and priority of the call, dispatch the appropriate response, then give the caller instructions to help treat the patient until the responding EMS unit arrives.

EMS
Emergency Medical Services. A type of emergency service dedicated to providing out-of-hospital acute medical care, transport to definitive care, and other medical transport to patients with illnesses and injuries which prevent the patient from transporting themselves.

EOL
End of Life. A term used by software and hardware vendors indicating that it is ending or limiting its support on the product and/or version to shift focus on their newer products and/or version.

ESInet
Emergency Services IP Network. An Internet Protocol (IP)-based inter-network (network of networks) shared by all agencies which may be involved in any emergency.

ESRI
Environmental Systems Research Institute. A supplier of GIS software, and geodatabase management applications.

FCC
Federal Communications Commission. The FCC is an independent federal agency responsible for regulating interstate and international communications by radio, television, wire, satellite, and cable in all 50 states, D.C. and U.S. territories. The FCC has adopted numerous regulations governing the provision of 9-1-1 services.

FEMA
Federal Emergency Management Agency. An agency of the U.S. DHS whose mission is to help people before, during, and after disasters.

FOIA
Freedom Of Information Act. A state or federal law that grants the public access to information possessed by government agencies. Typically, upon written request, agencies are required to release information unless it falls under an exemption.

GIS
Geographic Information System. A computer system to capture, store, manipulate, analyze, manage, and display all kinds of spatial or geographical data.

GPS
Global Positioning System. A satellite-based global navigation system that consists of (a) a constellation of 24 satellites in orbit 11,000 nmi above the Earth, (b) several on-station (i.e., in-orbit) spares, and (c) a ground-based control segment. The satellites transmit signals that are used for extremely accurate three-dimensional (latitude, longitude, and elevation) global navigation (position determination), and for the dissemination of precise time. GPS-derived position determination is based on the arrival times, at an appropriate receiver, of precisely timed signals from the satellites that are above the user's radio horizon.

GUI
Graphical User Interface. An interface through which the user interacts with electronic devices such as computers and smartphones.

HTTP
Hyper Text Transfer Protocol. The protocol is used for transferring user page requests as well as the pages that are returned by the Web server.

HTTPS
Hyper Text Transfer Protocol Secure sockets. Encrypts and decrypts user page requests as well as the pages that are returned by the Web server. The use of HTTPS helps to protect against eavesdropping and man-in-the-middle attacks.

IBR
Incident Based Reporting. See NIBRS.

ICAM
Identity, Credential, and Access Management. Represents the intersection of digital identities, credentials, and access control into one comprehensive approach.

ICO
9-1-1 Implementation and Coordination Office. The National Telecommunications and Information Administration and National Highway Traffic Safety Administration within the U.S. Department of Transportation are responsible for the joint 9-1-1 Implementation and Coordination Office (ICO). The ICO is required to facilitate coordination and communications among public and private stakeholders at local, state, tribal, federal, and national levels; administer a grant program for the benefit of 9-1-1 call centers across the country; and author or consult on several reports to Congress.

IDPS
Intrusion Detection and Prevention. A network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits.

IETF
Internet Engineering Task Force. One of the task forces (with more than 40 working groups) of the Internet Architecture Board, responsible for solving short-term engineering needs of the Internet.

IM
Instant Message. A computer based message sent directly from one user to another.

IMS
IP Multimedia Subsystem. A standards-based architectural framework for delivering multimedia communications services such as voice, video, and text messaging over IP networks.

Interoperability
The term 'interoperable' or 'interoperability' means the capability of ECCs to receive 9-1-1 requests for emergency assistance and information and data related to such requests, such as location information and callback numbers from a person initiating the request, then process and share the 9-1-1 request for emergency assistance and information and data related to such requests with other ECCs and responders in the field without the need for proprietary interfaces and regardless of jurisdiction, equipment, device, software, service provider, or other relevant factors.

IoT
Internet of Things. Refers to the ever-growing network of physical objects that feature an IP address for internet connectivity, and the communication that occurs between these objects and other Internet-enabled devices and systems.

IP
Internet Protocol. A Department of Defense (DoD) standard protocol designed for use in interconnected systems of packet-switched computer communication networks. Note: The internet protocol provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed-length addresses. The internet protocol also provides for fragmentation and reassembly of long datagrams, if necessary, for transmission through small-packet networks.

IRR
Instant Recall Recording. Records audio from telephone and radio allows users to play back conversations on demand.

IT
Information Technology. The study or use of systems (especially computers and telecommunications) for storing, retrieving, and sending information.

ITU
International Telecommunication Union. A specialized agency of the United Nations (UN) that is responsible for issues that concern information and communication technologies.

JSON
Java Script Object Notation. A lightweight data-interchange format.

JPG or JPEG
Joint Photographic Experts Group. A file type for images and a means of compressing an image.

MDT/C
Mobile Data Terminal/Computer. A computerized device used in emergency vehicles, such as police cars, to communicate with an ECC. They are also used to display mapping and information relevant to the tasks and actions performed by the vehicle such as CAD drawings, diagrams, and safety information.

MMS
A standard way to send messages that extends the core SMS (Short Message Service) capability to include multimedia content to and from a mobile phone over a cellular network.

NAS
Network Attached Storage. A file server that connects to a network.

NCIC
National Computer Information Center. A computerized index of criminal justice information maintained by the CJIS Division of the FBI.

NG9-1-1
Next Generation 9-1-1. The term 'Next Generation 9-1-1' means an interoperable, secure, IP-based system that (a) employs commonly accepted standards, (b) enables ECCs to receive, process, and analyze all types of 9-1-1 requests for emergency assistance, (c) acquires and integrates additional information useful to handling 9-1-1 requests for emergency assistance, and (d) supports sharing information related to 9-1-1 requests for emergency assistance among ECCs.

NGCS
Next Generation Core Services. The base set of services needed to process a 9-1-1 call on an ESInet. Includes the Emergency Services Routing Proxy (ESRP), Emergency Call Routing Function (ECRF), Location Validation Function (LVF), Border Control Function (BCF), Bridge, Policy Store, Logging Services, and typical Internet Protocol (IP) services such as Domain Name Server (DNS) and Dynamic Host Configuration Protocol (DHCP). The term Next Generation 9-1-1 (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 mission of the NHTSA, an agency of the U.S. Department of Transportation (DOT), is to save lives, prevent injuries, and reduce economic costs due to road traffic crashes, through education, research, safety standards, and enforcement activity.

NIBRS
National Incident-Based Reporting System. A CJIS program that captures detail on each single crime incident, as well as on separate offenses within the same incident, including information on victims, known offenders, relationships between victims and offenders, arrestees, and property involved in crimes.

NIST
National Institute of Standards. A part of the U.S. Department of Commerce (DOC) 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.

NOC
Network Operations Center. Ensures network infrastructure meets service level agreements, troubleshoots, and optimizes the network.

NIEM
National Information Exchange Model. An (eXtensible Markup Language (XML)-based information exchange framework for sharing data between communities of interest (COIs), across all levels of the United States government.

NPSBN
National Public Safety Broadband Network. A network that contains significantly more than a basic Third Generation Partnership Project (3GPP) Long Term Evolution (LTE) system. Traditional LTE Carrier networks provide connectivity from a device to the Internet or the Public Switched Telephone Network (PSTN). Public safety users need the NPSBN to be a complete system that provides nationwide, interoperable applications and services, in addition to connectivity to their agencies applications.

NTIA
National Telecommunications and Information Administration. NTIA is the Executive Branch agency that is principally responsible for advising the President on telecommunications and information policy issues. NTIA's programs and policymaking focus largely on expanding broadband Internet access. NTIA shares a joint office with NHTSA with responsibility 9-1-1 Implementation and Coordination Office (ICO).

NTP
Network Time Protocol. A protocol designed to synchronize the clocks of computers over a network.

ODBC
Open Database Connectivity. A standard application programming interface for accessing database management systems.

OJT
On the Job Training. Training of an employee after they are hired.

OSP
Originating Service Provider. A communications provider that allows its users or subscribers to originate 9-1-1 voice or non-voice messages from the public to the 9-1-1 authority.

OTT
Over-the-Top. Generally, refers to applications that operate on IP-based mobile data networks and that consumers can typically install on data-capable mobile devices.

PDP
Packet Data Protocol. A data structure that allows the device to transmit data using Internet Protocol.

P43
Broadband Implications for the Public Safety Answering Point (PSAP). Explores the impacts of broadband technology on the ECC and provide education, guidance, and focus to ECCs and 9-1-1 authorities for the benefit of the entire public safety community.

PEN
Penetration Testing. An authorized simulated attack performed on a computer system to evaluate its security.

PII
Personally Identifiable Information. Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

PMP
Project Management Plan. The formal approved document that defines the steps of the project.

PST
Public Safety Telecommunicator. The individual employed by a public safety agency as the first of the first responders whose primary responsibility is to receive, process, transmit, and/or dispatch emergency and non-emergency calls for service for law enforcement, fire, emergency medical, and other public safety services via telephone, radio, and other communication devices.

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.

PTP
Precision Time Protocol. A protocol used to synchronize clocks throughout a computer network.

QA/QI
Quality Assurance/Quality Improvement. All actions taken to ensure that standards and procedures are adhered to and that delivered products or services meet performance requirements.

Reliability
The term 'reliability or 'reliable' means the employment of sufficient measures to ensure the ongoing operation of NG9-1-1 including through the use of geo-diverse, device and network agnostic elements that provide more than one route between end points with no common points where a single failure at that point would cause all to fail.

RETAINS
Responsive Efforts to Assure Integral Needs in Staffing. A national study of staffing and retention issues in a random sample of public safety communications centers in 2004. A second study was conducted in 2005 to find out if staffing and retention issues were different in large centers (using the CALEA definition, a large center has 76 or more employees). The tools are research-based and designed specifically for public safety communications center managers.

RFI
Request For Information. A standard business process that has a purpose to collect written information about the capabilities of various suppliers. Normally it follows a format that can be used for comparative purposes.

RFP
Request For Proposal. A document that solicits proposal, often made through a bidding process, by an agency or company interested in procurement of a commodity, service, or asset, to potential suppliers to submit business proposals.

RMS
Records Management System. An agency-wide system that provides for the storage, retrieval, retention, manipulation, archiving, and viewing of information, records, documents, or files.

RTT
Real-Time Text. Allows text to be transmitted instantly as it is typed or created over Internet protocol (IP) networks. With RTT, there is no need to press a "send" key as there is for SMS texting.

SAAS
Software As A Service. A software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted. SAAS is typically accessed by users using a thin client via a web browser.

SAN
Storage Area Network. A network storage device that can be accessed by multiple computers.

SCP/SFTP
Secure Copy Protocol/SSH File Transfer Protocol. Protocols to transfer files via a Secure Shell connection. SFTP includes additional capabilities such as resuming broken connections.

SIP
Session Initiation Protocol. A communications protocol for signaling, for the purpose of controlling multimedia communication sessions. The most common applications of SIP are in Internet telephony for voice and video calls, private Internet Protocol (IP) telephone systems, as well as instant messaging over IP networks.

SLA
Service Level Agreement. Sets the expectations between the service provider and the customer and describes the products or services to be delivered.

SLTT
State, Local, Tribal, and Territorial. A domestic governmental entity.

SMS
Short Message Service. A service in Global System for Mobile communication (GSM) mobile telephony systems that allows the user to send and receive short (maximum 160-character) messages independently of voice calls; a nearly real-time service that stores messages in message centers if the receiving mobile telephone cannot be contacted. Note: SMS is both the handset function and the network service. SMS is used to inform users of pending voice messages, network outages, etc., but the principal use is in user-to-user messaging. Addressing is by telephone numbers (GSM only). Networks usually relay messages over network boundaries. There are gateways from e-mail and Web to SMS and from SMS to e-mail, but only on an experimental-service basis.

SNMP
Simple Network Management Protocol. An internet standard protocol used to monitor and manage network devices connected via IP networks.

SOC
Security Operations Center. Identifies and blocks cyber threats to the network.

SOUNDEX
A phonetic algorithm for indexing names by sound, as pronounced in English.

SOW
Scope of Work. Describes how the project goals will be achieved.

SS7
Signaling System Number 7. A set of protocols used to provide basic routing information, call set-up, and other call termination functions.

SSH
Secure Shell. A cryptographic network protocol for operating network services securely over an unsecured network.

SQL
Structured Query Language. A standardized programming language that is used to manage relational databases and perform operation on the data.

SYN Flood
Synchronized message to establish TCP connections is a type of denial-of-service attack (DDoS).

TCP/IP
Transmission Control Protocol/Internet Protocol. A suite of communications protocols used to interconnect network devices on the internet or private computer networks.

TFOPA
Task Force on Optimal PSAP Architecture (FCC). The FCC's Task Force on Optimal Public Safety Answering Point (PSAP) Architecture was directed to study and report findings and recommendations on structure and architecture in order to determine whether additional consolidation of ECC 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.

TTY/TDD
Teletypewriter / Telecommunications Device for the Deaf. A unique telecommunication device for the deaf, using TTY principles. A machine that uses typed input and output, usually with a visual text display, to enable individuals with hearing or speech impairments to communicate over a telecommunications network.

UCR
Uniform Crime Report. FBI report with an objective to generate reliable information for use in law enforcement administration, operation, and management.

UDP
User Datagram Protocol. A communications protocol to establish low-latency and loss-tolerating connections between applications on the internet.

USB
Universal Serial Bus. An external serial bus interface standard for connecting peripheral devices to a computer.

UTC
Universal Time Coordinated. A time standard commonly used across the world to keep time scales closely synchronized.

VoIP
Voice over Internet Protocol. Technology that permits delivery of voice calls and other real-time multimedia sessions over Internet Protocol (IP) networks. Communication services that originate or terminate via IP networks rather than the circuit switched Public Switched Telephone Network (PSTN).

VIN
Vehicle Identification Number. Composed of 17 characters, digits and capital letters, that act as a unique identifier for the vehicle.

VPN
Virtual Private Network. A method employing encryption to provide secure access to a remote computer over the Internet.

WAN
Wide Area Network. Is a large network of information that is not tied to a single location.

WMV
Windows Media Video. A compressed video file format developed by Microsoft.

XML
eXtensible Markup Language. A trimmed specification or version of the Standard Generalized Markup Language (SGML) that allows Web developers to create customized tags for additional functionality.

Index

M

N

O

P

Q

R

S

T

V

W

APCO International®

ABOUT APCO

APCO International is the world's oldest and largest organization of public safety communications professionals and supports the largest U.S. membership base of any public safety association. It serves the needs of public safety communications practitioners worldwide – and the welfare of the general public as a whole – by providing complete expertise, professional development, technical assistance, advocacy and outreach.

APCO International
351 N. Williamson Blvd.
Daytona Beach, FL 32114

www.apcop43.org