INSTITUTE FOR DEFENSE ANALYSES

Department of the Army: Closing the Next Generation 9-1-1 Capability Gap

Serena Chan, *Project Leader*
Michael T. Hernon

May 2019

IDA Document
D-10648

INSTITUTE FOR DEFENSE ANALYSES
4850 Mark Center Drive
Alexandria, Virginia 22311-1882

The Institute for Defense Analyses is a non-profit corporation that operates three federally funded research and development centers to provide objective analyses of national security issues, particularly those requiring scientific and technical expertise, and conduct related research on other national challenges.

About This Publication

This work was conducted by the Institute for Defense Analyses (IDA) under contract HQ0034-14-D-0001, Task BC-5-4012, "DoD NG9-1-1 Transition and Connection to State ESINets," for HQDA OPMG. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgments

Gregory N. Larsen, Francisco L. Loaiza-Lemos

For more information:

Serena Chan, Project Leader
schan@ida.org, 703-933-6563

Margaret E. Myers, Director, Information Technology and Systems Division
mmyers@ida.org, 703-578-2782

INSTITUTE FOR DEFENSE ANALYSES

IDA Document D-10648

Department of the Army: Closing the Next Generation 9-1-1 Capability Gap

Serena Chan, *Project Leader*

Michael T. Hernon

Executive Summary

This document reports on work done by the Institute for Defense Analyses (IDA) for the U.S. Army Office of the Provost Marshal General (OPMG) and for the Office of the Deputy Chief Information Officer (DCIO) for Command, Control, Communications and Information (C3I), Department of Defense (DoD) Chief Information Officer (CIO). National public safety leaders and industry are focused on rapidly accelerating the deployment of Next Generation 9-1-1 (NG911) by the end of year 2020. It is crucial for DoD emergency call centers to migrate to NG911 in concert with their host U.S. states and territories.

The overall objective of this work was to recommend courses of action to the Army as it considers upgrading to a digital or Internet protocol (IP)-based 9-1-1 system. This document addresses the need for the Army to migrate to a NG911 environment, describes the benefits of this migration and the risks to life and assets in not doing so, and makes several recommendations for next steps.

Migrating to NG911 will enhance the Army's capabilities to save lives and protect property. In addition to avoiding obsolescence, migrating to the new environment provides first responders and emergency management personnel with the following enhanced and new capabilities:

- Integrated end-to-end information flow
- Text, video, and imagery processing
- Enhanced location information
- Increased resiliency
- Interoperability with civilian mission partners
- Information sharing
- Enhanced mutual aid capabilities

These benefits have a direct, positive impact on several mission areas including Public Safety, Emergency Management, Force Protection, Anti-Terrorism, Mission Assurance, and Critical Infrastructure Protection.

NG911 is both an operational requirement and a strategic capability supporting multiple Army missions. Given the cross-cutting nature of this capability, it is desirable to have a proactive approach that will avoid obsolescence and deliver the benefits of the

NG911 environment as soon as practical. Table 1 provides recommendations for near-term actions required by the Army to start closing the NG911 capability gap.

Table 1. Recommendations

Recommendation	Discussion
Recommendation #1: ***Implement a governance body***	An overarching governance body and structure is needed to provide oversight and guidance for all activities involved in the transition. The governance scope should be enterprise-wide. As NG911 is a cross-cutting capability, stakeholders from all beneficiaries of the new environment should be represented on the governance body.
Recommendation #2: ***Develop an enterprise NG911 strategy***	A high-level NG911 migration strategy detailing specific goals and objectives should be developed by the governance body. The strategy should contain a policy analysis to identify any potential DoD or Army policy constraints that would require mitigation to facilitate deploying NG911.
Recommendation #3: ***Conduct a business case analysis (BCA)***	A detailed BCA utilizing the DoD BCA template should be conducted. The analysis of alternatives in the BCA should include traditional, hybrid, and NG911 as-a-service options with estimated procurement costs for each.
Recommendation #4: ***Complete geographic information system (GIS) enhancements***	The ongoing GIS enhancements should ensure that all locations of interest, addresses, building identifiers, etc., are fully geocoded with *x* and *y* coordinates. Installation-level GIS should follow NENA i3 guidelines to maximally support NG911. GIS data at the For Official Use Only (FOUO) level and below should be integrated with the shared next-generation mapping services of the surrounding jurisdictions.
Recommendation #5: ***Develop and execute a deployment strategy***	Based on the results of the BCA, a deployment strategy, including the acquisition of the solution, can be developed and executed. Memorandums of Understanding (MOUs) and other agreements with civilian agencies would also need to be executed if required. This is the last requirement to exit the Foundational State and enter the Intermediate State.

Contents

Figures

Tables

1. Introduction

This document reports on work done by the Institute for Defense Analyses (IDA) for the U.S. Army Office of the Provost Marshal General (OPMG) and for the Office of the Deputy Chief Information Officer (DCIO) for Command, Control, Communications and Information (C3I), Department of Defense (DoD) Chief Information Officer (CIO). National public safety leaders and industry are focused on rapidly accelerating the deployment of Next Generation 9-1-1 (NG911) by the end of year 2020. It is crucial for DoD emergency call centers to migrate to NG911 in concert with their host U.S. states and territories.

This document addresses the need for the Army to migrate to the NG911 environment, describes the benefits of this migration and the risks to life and assets in not doing so, and makes several recommendations for next steps, including conducting a detailed business case analysis coupled with an analysis of alternatives, to determine the optimal deployment strategy across the Army enterprise.

A. Background

As in other areas of technology, today's analog-based 9-1-1 solutions are reaching end-of-life and are being replaced by solutions based on digital technology. Hence, the technology underlying the way that public safety entities receive, process, and respond to 9-1-1 calls requires updating or replacement. Similar migrations are underway in Europe (NG112) and other locations worldwide where the Army maintains installations. This migration is in response to the commercial carriers replacing legacy, analog-based voice networks with an environment based entirely on digital, Internet protocol (IP)-based communications.

This new environment has been defined at a functional level by the National 911 Program at the U.S. Department of Transportation. A variety of technical standards for deploying NG911 systems and services have been developed and published by the National Emergency Number Association (NENA) in collaboration with key stakeholders. These "i3" standards have been universally adopted, and original equipment manufacturers are now producing NG911 i3-compliant components and solutions.

As reported in the *2017 National 911 Progress Report* of November 2017, two-thirds of states housing major Army installations had statewide NG911 programs in place (see Appendix A). Of those states, almost half had deployed some of their 9-1-1 call centers or

public safety answering points (PSAPs) onto the Emergency Services IP network (ESInet) in lieu of the legacy 9-1-1 phone network. These numbers have grown significantly, as that report was based on 2016 data. ESInets are also being deployed at the sub-state, regional, and even at the inter-state level. For example, in the National Capital Region, 17 jurisdictions including the District of Columbia and PSAPs in Maryland and Virginia will have three interconnected ESInets and share common NG911 core services over that architecture.

What civilian and other federal first responder organizations do in their NG911 migrations is critical to Army PSAP operations and first responders, as numerous mutual aid agreements exist between Army and non-Army organizations. These outside organizations are key civilian mission partners, and these agreements define how non-Army first responders support emergency operations on Army installations, and vice versa. This support occurs daily for "routine" emergencies, such as an Arlington County, VA, ambulance responding to the Pentagon, as well for major incidents, such as those that occurred at Fort Hood in 2009 that entailed a massive response by local government first responders. Army first responders similarly respond to routine calls for service outside their installation, as well as execute large-scale deployments for major incidents such as the western wildfires. Both types of mutual aid will be severely constricted if the legacy Army 9-1-1 infrastructure prohibits or constrains emergency operations with these mission partners.

The ongoing migration to NG911 among Army mission partners and the looming retirement of the analog 911 environment represents a significant and growing capability gap for the Army's public safety/emergency management community of practice. Closing the gap requires a similar migration by the Army. This migration aligns with Department of Defense (DoD) and Army strategies, including the *Army Network Campaign Plan* (*ANCP*) for network modernization across all of its domains: network capacity, enterprise services, and network operations and security. Ensuring the migration is also conducted in accordance with NG911 standards and Federal Communications Commission (FCC) guidance will close the capability gap and significantly enhance the mission partner environment.

B. Scope

This document's analysis leverages and builds upon the *Computer Aided Dispatch Capability Problem Statement* released on June, 18, 2015, hereafter referred to as the *CAD Problem Statement*, and included herein as Appendix C. As of this writing, the to-be state described in that document has been partially achieved. Delivering those to-be state

capabilities[1] is still required, with an extension for the provision of NG911 capabilities, to enable the to-be state described in this document and close the capability gap.

Given the critical nature of this capability, this document recommends a proactive approach to avoid obsolescence and deliver the benefits of the NG911 environment as soon as feasible with a comprehensive, enterprise-wide strategy guiding the acquisition and deployment of NG911 capabilities.

[1] The to-be state in the *CAD Problem Statement* envisioned a single enterprise solution providing the capabilities. In this analysis, we stress delivering an enterprise capability, that may, or may not, be delivered via a single solution.

2. As-Is Analysis

Much of the current 9-1-1 call handling equipment (CHE) and computer-aided dispatch (CAD) capability of the Army relies on outdated equipment. Readers are referred to Appendix C, the *CAD Problem Statement*, for a complete description of the as-is environment as of 2015.

A. Problem Description

The end-to-end lifecycle of an emergency call for service can be viewed as being composed of three distinct components, albeit with many subsystems:

- the incoming 9-1-1 call (or input from other sources such as a sensor or an alarm),
- the response formulation/dispatch process, and
- field operations support and communications.

Each of these components relies on a specialized suite of equipment and software. Figure 2-1 shows a high-level view of the legacy architecture in place today.

1. Incoming Call for Service

A 9-1-1 call is typically the first action an individual takes in an emergency to request police, fire, or emergency medical services (EMS) assistance. In the U. S., 9-1-1 has been the universal emergency telephone number since the FCC mandated its use in 1999; however, its use had been growing since its inception in 1968. Over the ensuing years, a broad, robust 9-1-1 architecture in the public switched telephone network (PSTN) was developed to ensure that emergency calls were given special handling in the phone system and that the calls were delivered to the appropriate PSAP in a reliable way. These advances include the use of dedicated 911 telephony trunks, automated number identification, automated location information, or Enhanced 9-1-1 (E911), and the use of selective routers, to name a few. More recently, FCC guidelines dedicated to wireless 9-1-1 calls have also been enacted, primarily around providing location information.

Although the FCC rulings on 9-1-1, E911, and other related capabilities do not apply to the DoD, the Department did eventually mandate the deployment of E911 in accordance

with the lessons learned from the Fort Hood attacks.[2] The requirement today is established in DoD Instruction 6055.17, *DoD Emergency Management Program*. DoD policy currently under coordination will also require alignment with all relevant FCC rulings, prevalent civilian best practices and standards, as well as a migration to NG911.

After having basic location information appended (if available), the 9-1-1 call is routed to the appropriate PSAP. For wireless calls, which comprise 80% of all 9-1-1 calls today, the caller will be routinely routed to the jurisdiction where the cell tower is located, which may not be the same as the caller's location (as on an Army installation). Whatever the source, the call is received by a call taker utilizing CHE, a combination of specialized hardware and software applications dedicated to the handling of 9-1-1 calls.

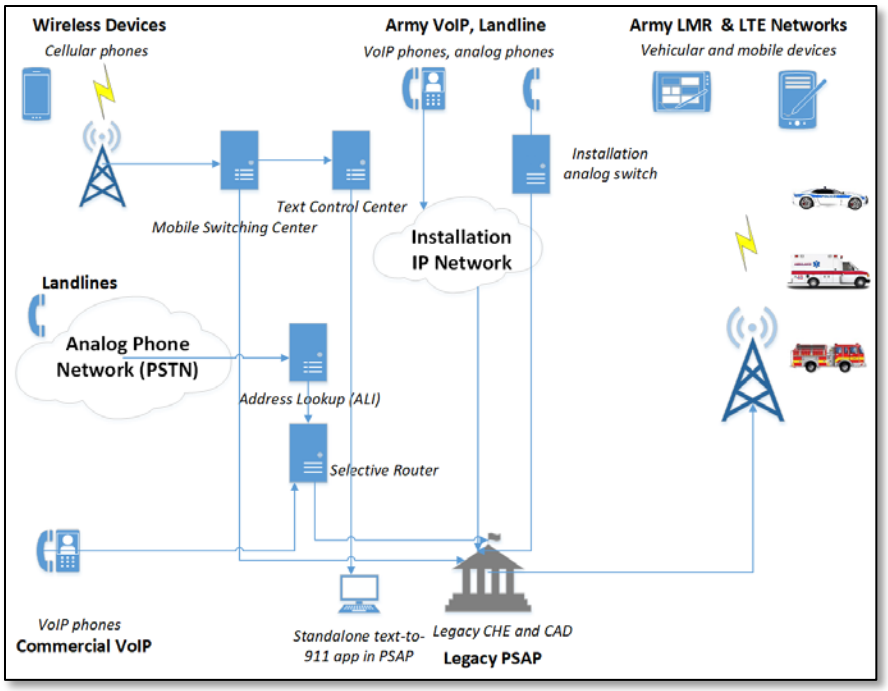


Figure 2-1. High-Level 9-1-1 Architecture

If an incident is validated, then the call taker forwards the CHE information to the CAD environment. In some Army locations, the CHE and CAD were acquired as a single solution from one vendor, as with the Intergraph I/CAD systems recently deployed. In others, the CHE and CAD were acquired and deployed separately, as with those locations

[2] SECDEF memorandum *Final Recommendations of the Ft. Hood Follow-on Review,* August 18, 2010, mandated E911 across all installations, in accordance with the recommendations of the Fort Hood independent review of an active shooter event at the fort in 2009, which claimed 13 lives.

using a VESTA-brand CHE paired with another vendor's CAD solution, or used alone as a call-handling solution without a CAD capability.

2. Computer-Aided Dispatch

The CAD system is the heart of first responders' ability to quickly and effectively respond to a call for service. The CAD system receives basic incident information input from the CHE and assists in determining the optimal response and in providing dispatch and ongoing incident management support. CAD systems are highly complex and consist of a number of automated subsystems that assist in determining the type of response, the number and type of units for dispatch, and the first responder skill sets required, among many other functions. CAD systems are typically richly interconnected with a variety of outside systems such as records management systems, land mobile radios (LMRs), and mobile computing devices.

The CAD environment in the Army today is bifurcated between the legacy environment described in the *CAD Problem Statement* and the Intergraph I/CAD 9.4 solution deployed more recently.

3. Army Legacy CAD Environment

Most Army installations operate under the legacy environment. This includes 41 installations without any CAD capability. Given the vital role CAD plays in emergency response, this lack significantly increases the level of risk to an installation's population. One measure of this is the inability of many of these installations to meet Installation Management Command (IMCOM) Common Level of Service (CLS) requirements as documented in the *CAD Problem Statement*.

Although installations with a CAD capability were shown to provide a better level of service as measured by CLS performance, the significant shortcomings described in 2015 remain today. These include locally procured systems with no overarching acquisition strategy, lack of E911, cybersecurity vulnerabilities, lack of interoperability, lack of information sharing, inadequate connectivity to other systems, inability to comply with relevant DoD and Army policies, and minimal or a complete lack of wireless capabilities. These shortcomings translate to a variety of operational and efficiency constraints with the end result being a capability that underperforms while costing more than it should.

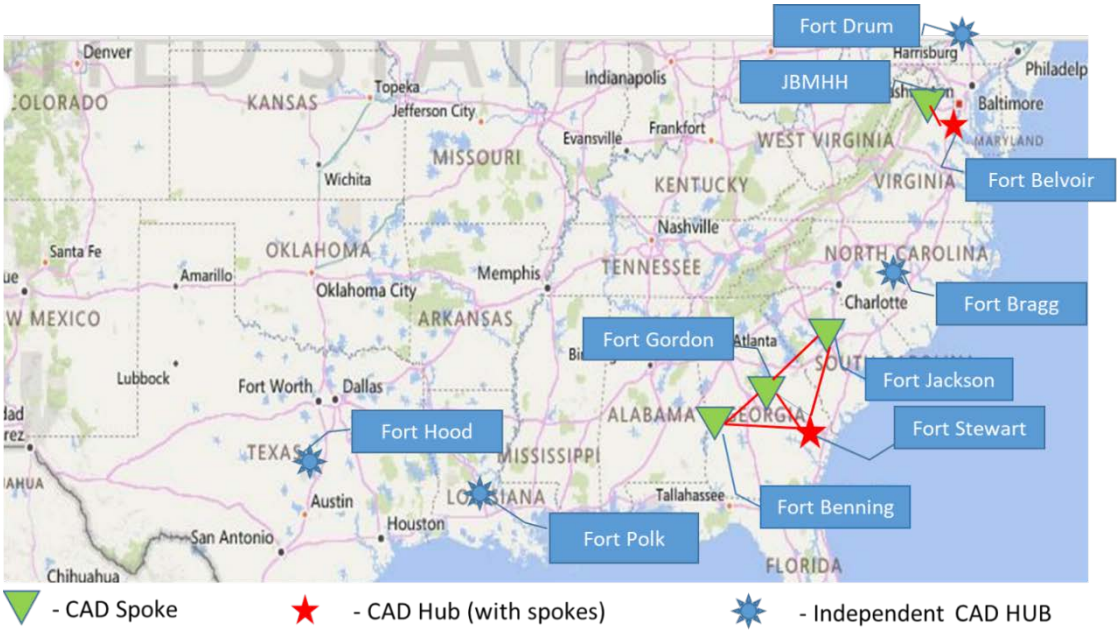
4. I/CAD Environment

As a result of the *CAD Problem Statement*, funding was allocated to support an enterprise CAD approach to alleviate the shortcomings described above. The selected solution was the Intergraph I/CAD product, version 9.4, from Hexagon Safety and Infrastructure. For this deployment, the CAD is integrated with the CHE, obviating the

need to acquire that component separately and ensuring that the CHE and CAD systems remain in sync with future vendor upgrades.

As of this writing, the I/CAD solution has been deployed to 10 installations, with two more currently under consideration (see Figure 2-2). The 10 installations are as follows:

- Fort Belvoir
- Fort Benning
- Fort Bragg
- Fort Drum
- Fort Gordon
- Fort Hood
- Fort Jackson
- Fort Polk
- Fort Stewart
- Joint Base Myer-Henderson Hall



Note: Reprinted from Army PEO EIS presentation *PSAP Assembly*, February 7-8, 2017.

Figure 2-2. Installations with I/CAD 9.4 Deployed

Where feasible, a hub-and-spoke infrastructure was used in the deployment, resulting in two hub installations serving four spoke installations. In this model, a hub location contains the traditional CAD computer environment that serves one or more spoke locations using virtual machines. This delivers a range of advantages to the Army including cost savings from a variety of sources, elimination of redundant equipment, standardization, and facilitation of a Common Operating Picture (COP). The hub-and-spoke deployment also supports the computing services objective to consolidate computing and storage infrastructure outlined in the *ANCP*. Four installations were provided with standalone CAD systems.

In addition to CAD and CHE, the solution being fielded also includes mobile CAD so that first responder vehicles will have full CAD access and support in the field.

5. Operational Support and Communications

The last link in the response chain is the actual dispatching of, and ongoing communications with, the first responders by PSAP personnel. This is primarily accomplished today using LMR networks and some mobile data computers (MDCs) mounted in the emergency vehicles integrated into the CAD. These typically operate over private LMR networks and commercial cellular networks, respectively. Although these first responder systems are outside the scope of NG911, the NG911 environment will nonetheless significantly enhance these capabilities as well.

B. DOTMLPF-P Constraints

The as-is environment results in several shortcomings across the doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) spectrum as summarized in Table 2-1.

Table 2-1. DOTMLPF-P Constraints on "As-Is" State

Category	Shortcoming
Doctrine	• Doctrine is developed and maintained individually at the Installation level.
Organization	• Up to 73 installations affected belong to IMCOM, Medical Command (MEDCOM), Training and Doctrine Command (TRADOC) and Army Medical Command (AMC).
Training	• There is no training program for NG911.
Materiel	• Much of the inventory is incapable of supporting the NG911 environment, although recently purchased CHE and CAD may be able to be upgraded. • Current data networks are unable to provide ESInet or NG core services.
Leadership and Education	• Decisions are made locally at the installation Provost Marshal level. Though levels of service are outlined by IMCOM, there is not a standardized approach to meeting them.
Personnel	• Qualified personnel are hired through the General Schedule system and are trained on the individual solution at their installation.
Facilities	• Buildings supporting call taking and emergency dispatch services have additional security concerns and restrictions; relevant systems are separated from other IT systems.
Policy	• DoDI 8320.07, an information sharing policy, outlines data sharing over DOD systems and with mission partners. Current systems are not able to adhere to these standards. • DoDI 8330.01, an interoperability policy, requires the use of interoperable systems with mission partners. The current environment does not meet this requirement. • DoDI 8540.01, a cross-domain policy, directs that cross-domain solutions be developed to meet mission requirements. The legacy environment cannot meet this requirement. • AR 420-1, *Army Facilities Management*, addresses fire dispatch and response standard. However, AR 190-45, *Law Enforcement Reporting*, does not provide the same for police. • IMCOM CLS provide the current standards that installations must meet with their current systems. Non-standardized systems currently meet only some of these requirements, depending on the installation. • AR 70-1, *Army Acquisition Policy*, requires that Army-controlled systems must use a system of systems approach that leverages aspects of the Chief Information Officer/G-6 (CIO/G-6) and Assistant Secretary of the Army (Acquisition, Logistics and Technology (ASA (ALT)) Common Operating Environment (COE) Architecture and the DOD IT Strategy Roadmap. The legacy environment does not comply.

C. As-Is State Summary

The as-is environment represents a major impediment to Army first responder operations. The shortcomings of the as-is state will only become more problematic as NG911 becomes prevalent among the civilian mission partners and the legacy commercial networks are retired by the providers.

Most of the outdated equipment that is prevalent in the as-is state will not be capable of being upgraded to NG911 and will need replacement. However, equipment installed in the past few years as a result of the *CAD Problem Statement* and ensuing modernization program should be capable of being upgraded. This will require some new components and updated software versions supporting NG911 but would not likely require a wholesale replacement of the equipment itself.

The Intergraph product is one of the most widely adopted CAD solutions in the U.S., and represents a necessary first step in closing the capability gap and modernizing the solution in accordance with the *ANCP*. It has a particularly strong mapping component due to Intergraph's long history as a leader in geographic information systems (GIS). Its adoption by the Army has significantly addressed the shortcomings of the legacy environment. However, for the most part, the legacy environment described in the *CAD Problem Statement* remains prevalent across Army installations. Additionally, I/CAD 9.4 as deployed is not an NG911 platform. As a result, the entire as-is environment must migrate to the new standard through either upgrading or replacing current equipment as well as adding additional NG911 components.

Lastly, the as-is environment is at end-of-life, and is not sustainable. At some point in the not-too-distant future, the legacy, analog telecommunications networks will be retired by the commercial providers[3]. When that occurs, only an IP-based NG911 solution could support the Army's first responders.

[3] Each state's public utilities commission, or similar body, is overseeing this process under overarching FCC guidance. As such, the schedule may vary among states. Virginia, for example, has adopted June, 2023 as the date for which all 9-1-1 selective routers will have been decommissioned. Regions within the state will see earlier terminations as routers will be retired when the PSAPs they serve complete their ESInet migration.

3. To-Be State

A. Overview

The NG911 environment, the "to-be" state, represents both a necessary transition from the as-is state as well as a quantum leap in capabilities. NG911 will remove the current constraints imposed upon the Army by the legacy environment and provide a level of service that is commensurate with the best civilian agencies.

B. NG911 Defined

The major stakeholder organizations define NG911 as follows:[4]

Next Generation 9-1-1 services means a secure, IP-based, open-standards system comprised of hardware, software, data, and operational policies and procedures that:

1) *Provides standardized interfaces from emergency call and message services to support emergency communications;*
2) *Processes all types of emergency calls, including voice, text, data and multimedia information;*
3) *Acquires and integrates additional emergency call data useful to call routing and handling*
4) *Delivers the emergency calls, messages and data to the appropriate public safety answering point and other appropriate emergency entities based on the location of the caller*
5) *Supports data, video, and other communications needs for coordinated incident response and management; and*
6) *Interoperates with services and networks used by first responders to facilitate emergency response*

As the above definition shows, NG911 delivers more and richer data to public safety professionals and will substantially enhance the Army's capabilities to save lives and protect property.

In addition to avoiding obsolescence through the migration, the new environment also provides enhanced and new capabilities for first responders and emergency management personnel as described below.

[4] National 911 Program, *Next Generation 911 Interstate Playbook*, June 2018.

C. To-Be State Benefits

The benefits of the to-be state include the following:

- ***Integrated end-to-end information flow.*** Data coming from the 9-1-1 caller, or other system input, is available throughout the life cycle of the incident and can pass from CHE, to CAD, to first responders as required. The data is maintained after the incident and kept available through a records management system (RMS) for analysis and to meet record-keeping requirements.
- ***Text, video, and imagery processing***. The system supports multiple data types, such as video feeds or images from a caller's cell phone. This data is also maintained in the RMS as appropriate.
- ***Enhanced location information***. NG911 can determine a caller's location with a much higher degree of fidelity and can route wireless emergency calls in a more intelligent manner than today's systems.
- ***Increased resiliency***. The native ability to seamlessly interconnect PSAPs provides more robust backup and continuity of operations (COOP) capabilities.
- ***Interoperability with civilian mission partners***. As all NG911 systems are based on the same set of NENA i3 standards, interoperability between organizations, even using different vendors' solutions, is an inherent capability.
- ***Information sharing***. NG911 systems are based on a common set of database structures and definitions that facilitate information sharing within, and external to, the organization.
- ***Enhanced mutual aid capabilities***. CAD-to-CAD connections and conferencing capabilities with mission partners will facilitate mutual aid operations and the provision of a shared COP.
- ***Operational flexibility***. As the FCC's Task Force on Optimal PSAP Architecture states, "NG9-1-1 architecture can be customized to support almost any configuration of PSAP operations." [5] This gives the Army the ability to support its hub-and-spoke model while also supporting different configurations if required by the needs of a particular installation.

NG911 capabilities and benefits directly align to and support the Army's implementation of the Federal Emergency Management Agency's (FEMA) preparedness model, particularly the Response component, as adopted across the DoD in accordance with DoD Instruction 6055.17, *DoD Emergency Management*.

[5] FCC Task Force on Optimal PSAP Architecture, *Adopted Final Report*, January 29, 2016.

These benefits have a direct, positive impact on several Army missions:

- Public safety
- Emergency management
- Force protection
- Anti-terrorism
- Mission assurance
- Critical infrastructure protection

Although the public safety community of practice will be the primary users of NG911, the system will also provide significant support to emergency managers by supplying feeds into WebEOC and similar emergency operations center (EOC) platforms. In addition, the system will deliver overall support to emergency management personnel.

The environment will also serve as an early warning indicator for other mission areas that protect people, missions, and critical assets across the Army enterprise. As such, NG911 is both an operational requirement as well as a cross-cutting strategic capability supporting multiple, critical Army missions.

Legacy CHE and CAD systems were not designed to support this new environment and are incapable of doing so. This is not surprising as the NG911 database definitions, interface requirements, and multimedia support (among other capabilities) did not exist when the legacy equipment was manufactured.

D. NG911 Architecture Overview

The main components of the NG911 environment include the following:

- Public IP networks supporting commercial cellular and VoIP networks. With the rise of 5G wireless services, the number and variety of devices that could interface with the 9-1-1 system is expected to expand dramatically.
- An installation IP network, which represent the on-base network that supports VoIP phones and other IP traffic.
- The Next Generation Core Services (NGCS), which provide the suite of NG911 functional capabilities.
- ESInet, which is the dedicated public safety network processing incoming 9-1-1 calls and other inputs and delivering the NGCS.
- Army LMR and LTE networks, which are the private LMR and commercial cellular networks providing voice and data capabilities to first responders.

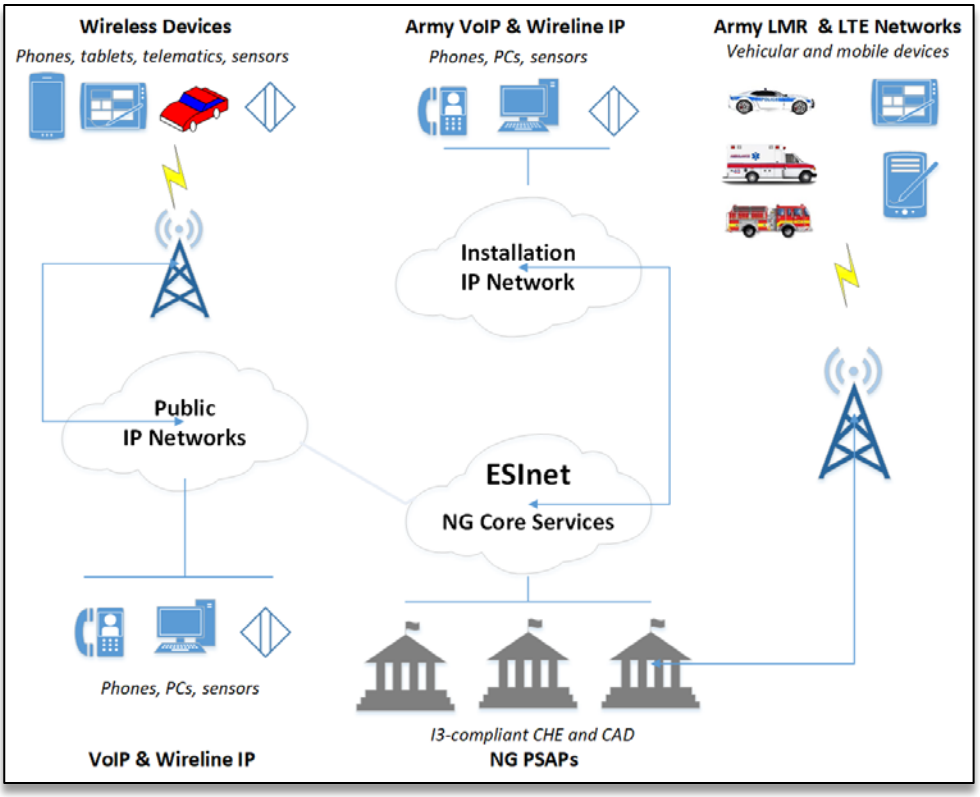


Figure 3-1. NG911 High-level Architecture

E. Call Handling Equipment & Computer-Aided Dispatch

The functionality of the CHE and CAD systems described in the *CAD Problem Statement* "to-be" state will be maintained in the NG911 environment, albeit with a different underlying architecture, and with the added functionality of NG911.

All current CHE systems must be either upgraded or replaced in order to receive 9-1-1 calls in an NG911-compliant manner. Later-model VESTA equipment in the Army inventory can be upgraded through the addition of an ESInet Integration Module, although older equipment would need to be replaced.

The CAD systems currently in the Army inventory will likewise need to be upgraded (recent Intergraph acquisitions) or replaced to leverage the NG911 environment and core services. As with the CHE, many of these services for CAD entail richer data sources that legacy CAD systems were not designed to accommodate.

It is important to note that moving 9-1-1 calls from Time Division Multiplexing (TDM) to IP is substantially different than a normal VoIP migration due to the special requirements and services that are entailed in an emergency call for service. To benefit

from the NG911 environment, a 9-1-1 call placed from a VoIP phone on an installation should also be routed through the ESInet.

F. Emergency Services IP Network

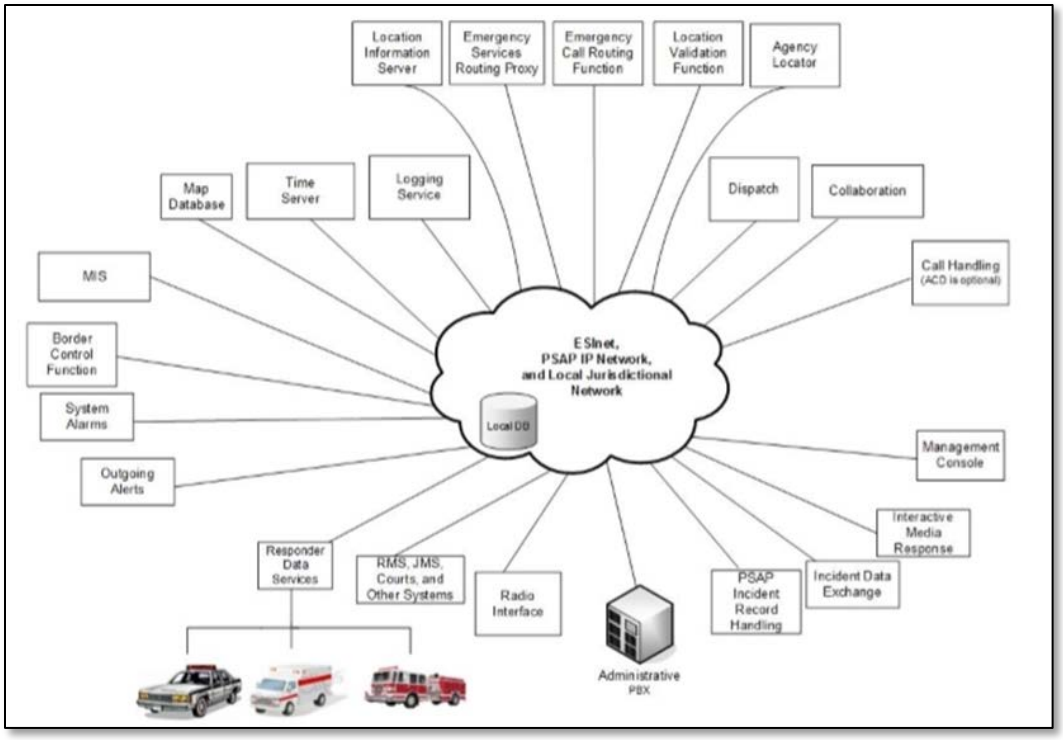
The ESInet is a public safety network dedicated to the delivery of NG core services to NG-compliant PSAPs and represents the IP-based replacement for the legacy 9-1-1 telephony components of the analog PSTN. ESInets are built to the NENA i3 standards.

One of the NENA i3 design requirements for the ESInet is to enable interoperability and connectivity among PSAPs in different locations and jurisdictions, even if they are operating on different CHE and CAD systems. This is not feasible in the as-is environment without complex, expensive, and bespoke interfaces. This universal standard facilitates ESInets and core services being deployed as a shared asset across multiple jurisdictions. This brings several operational efficiencies in transferring calls, sharing information, having access to a broader map, and assisting in mutual aid operations. It also brings financial savings as the costs are distributed across multiple user organizations. Resiliency is also enhanced, as any PSAP on the ESInet has the ability to serve as a backup for any other.

ESInet access for the Army supports the Information Transport capability of the *ANCP* as a component of the installation infrastructure modernization objective.

G. Next Generation Core Services

NGCS is a suite of applications responsible for call routing, location information, security and other key services that are currently provided for in the analog world. Access to these services is required for the NG911 environment to operate. Figure 3-2 shows how these core services and the ESInet combine to provide end-to-end emergency call support. The individual core services and their functions are listed in Table 3-1.



Note: Reprinted from NENA/APCO *Next Generation 9-1-1 PSAP Requirements*, April 5, 2018.

Figure 3-2. NG911 Functional Overview

Table 3-1. NG Core Services

Location Information Server	Provides the location of the IP input (9-1-1 call or other input mode).
Location Validation Function	Determines if the presumed location is a true, dispatchable address (or geo-coordinates). Updates location during the life of the call.
Emergency Services Routing Proxy	Determines which node on the ESInet should next receive the call for service based on policy.
Emergency Call Routing Function	Determines which PSAP is the ultimate receiver of the call.
Agency Locator	A lookup table with contact info for all agencies sharing the ESInet.
Map Database	Database of GIS-produced maps of all geography covered by the ESInet.
Time Server	Provides all nodes on the ESInet with extremely accurate time input to support standardization and synchronization.
Logging Service	ESInet- or PSAP-based repository of all IP input related to a call.
Dispatch	Supports dispatchers in their role.
Collaboration	Provides a suite of collaboration tools for users on the ESInet.
Call Handling	Provides reception and processing of incoming calls and support for call taker functions.
Management Information System (MIS)	Overarching data management and reporting.
Border Control Function	Provides security for entry into the ESInet, includes firewall and associated capabilities.
System Alarms	Provides notification of system faults.
Outgoing Alerts	Manages all active alerts for responders.
PSAP Incident Record Handling	Processes incident data throughout the life cycle of the incident.
Incident Data Exchange	Provides the ability to forward incident data between systems within, and outside of, the agency
Interactive Media Response	Automated audio, video, or text communications with a caller.
Management Console	Provides general PSAP management tools.
Responder Data Services	Provides wireless communications from an NG911 CAD to mobile responder devices.
Radio Interface	Provides CAD-to-LMR interface.

H. Location-Based Services and Geographic Information Systems

Most CHE and CAD systems today rely, to some extent, on a mapping component using data from a more complex, off-line GIS. One of the significant life-saving improvements in the NG911 environment is the ability to provide enhanced location information to the call taker/dispatcher at a much more precise level than currently available, including *z*-axis data to indicate which floor in a building a caller is on.

Another advantage of NG911 location services is the ability of the system to route a wireless 9-1-1 call to the appropriate PSAP based on the actual location of the caller rather than the cell tower they are connected to. For example, any wireless 9-1-1 call made from an Army installation today will, more likely than not, connect to a commercial cell tower that is not located on the installation. Under today's technology, that call is routed to the local government jurisdiction where the tower is located, not the PSAP on the installation where the emergency call was placed from. Time is then lost in transferring the call to the Army PSAP. Also, information is also often lost as the ability to automatically transfer location and other relevant information along with the voice call itself is not universally available. Figure 3-3 shows the two routing practices in graphic format.

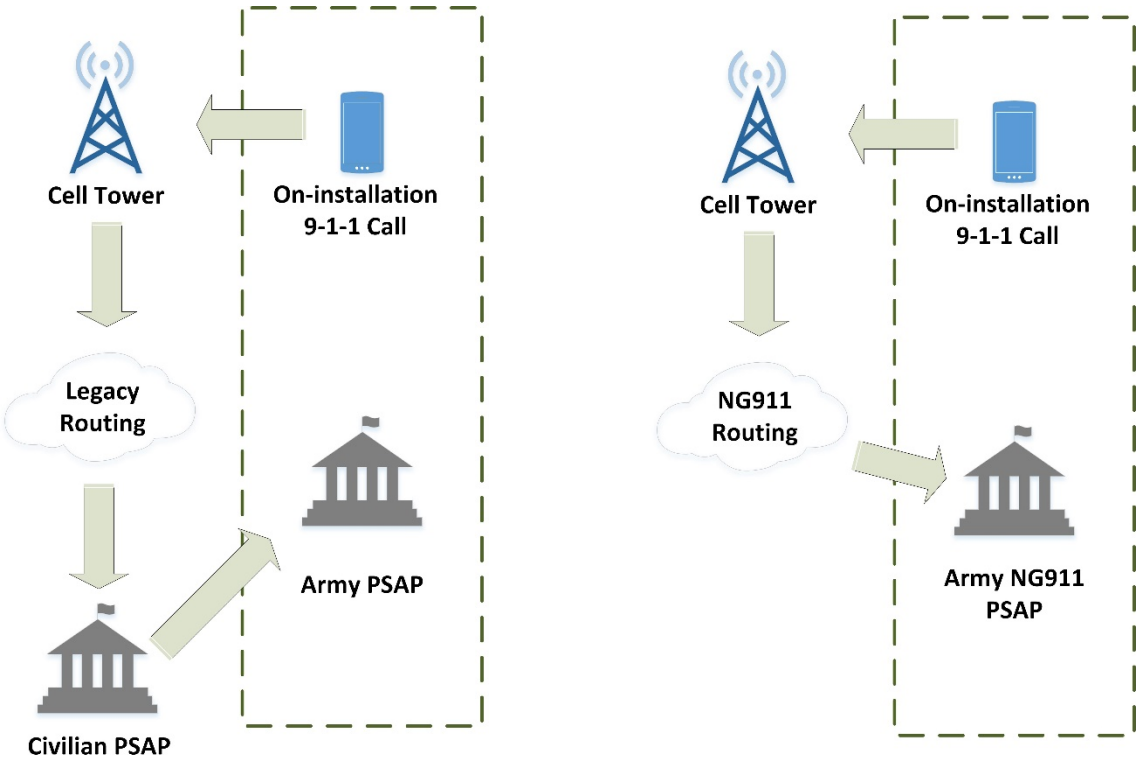


Figure 3-3. Legacy (L) and NG911 (R) Cellular Call Routing

Time lost in responding to a 9-1-1 call increases risk to life. The FCC estimates that the time saved just by providing enhanced location information would save over 10,000 lives in a year across the U.S.[6] To support these location-based services, NG911 relies much more heavily on the underlying GIS data than today's systems. Nearly all civilian jurisdictions are undertaking GIS upgrades as part of their NG911 migration strategy. A key GIS enhancement for NG911 is updating the Master Street Address Guide (MSAG) to include *x* and *y* coordinates for each address and key location and eliminating block-based addressing.

I. Ancillary Systems

Loggers and recorders that support CAD systems allow organizations to maintain records as required by law or local policy. They exist today in IP-capable versions that provide the same functionality in an NG911 environment. These existing systems may require an upgrade. Additional systems, such as Telecommunications Devices for the Deaf/Teletypewriter (TDD/TYY) systems, video and sensor feeds, and wireless first responder devices, may also need to be upgraded or re-configured to integrate into the NG911 CHE/CAD solution.

J. Operational Support

The data, including imagery and video, in a NG911 system can also be pushed to first responders as appropriate to facilitate their response and incident management. In the NG911 environment, LMRs are expected to remain the primary mode of voice communications for the near- to mid-term. The MDCs, however, would receive enhanced data flow from the mobile component of the NG911 CAD system.

Additional capabilities, including alternative voice modes, would be provided by hand-held devices operating on commercial or private LTE networks. These provide the mobile, data-on-foot capability providing increased situational awareness to the first responders during their operations. These devices and networks also support LMR-like push-to-talk and point-to-point communications as well as network priority and preemption for emergency personnel.

[6] See FCC report FCC14-13.

4. Capability Gaps

Analysis of the as-is environment compared to the to-be environment highlights several serious shortcomings resulting in a significant capability gap that will only grow over time if not addressed (see Table 4-1). The most salient gap between the environments is that the as-is environment is at end-of-life, whereas the to-be state is in its early adoption phase and will remain the standard for years to come.

Table 4-1. Capability Gap

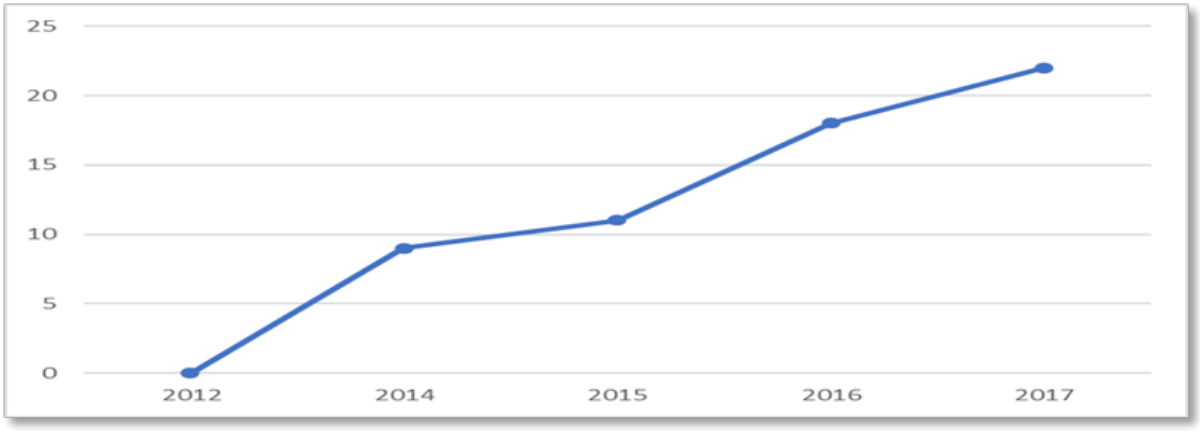
Measure	As-Is	To-Be (NG911)
Life Cycle Phase	End of life	Adoption
Architecture	Analog	Digital
Standards-based	No	Yes
DoD/Army Policy Compliance	No	Yes
Location: *X*, *Y* Axes	Approximate	Enhanced
Location: *Z* Axis	No	Yes
Text-to-911	No	Yes
Interoperable	No	Yes
Info Sharing	No	Yes
Multi-media Support	No	Yes

A. Mission Partner Environment Gap

In addition to the capability gap between the as-is and to-be environments, there is a real, and growing, capability gap between Army installations and their surrounding state and local jurisdictions. This gap presents significant operational barriers to effective mutual aid operations, thereby raising the risk to life and property. The 911 Program Office at the U.S. Department of Transportation has been tracking progress on the states' NG911 implementation since 2012. In their 2017 report (the latest available), they reported that 22 out of 47 responding states/territories had installed and tested NG911 and, in many cases, are using NG911 to process emergency calls.

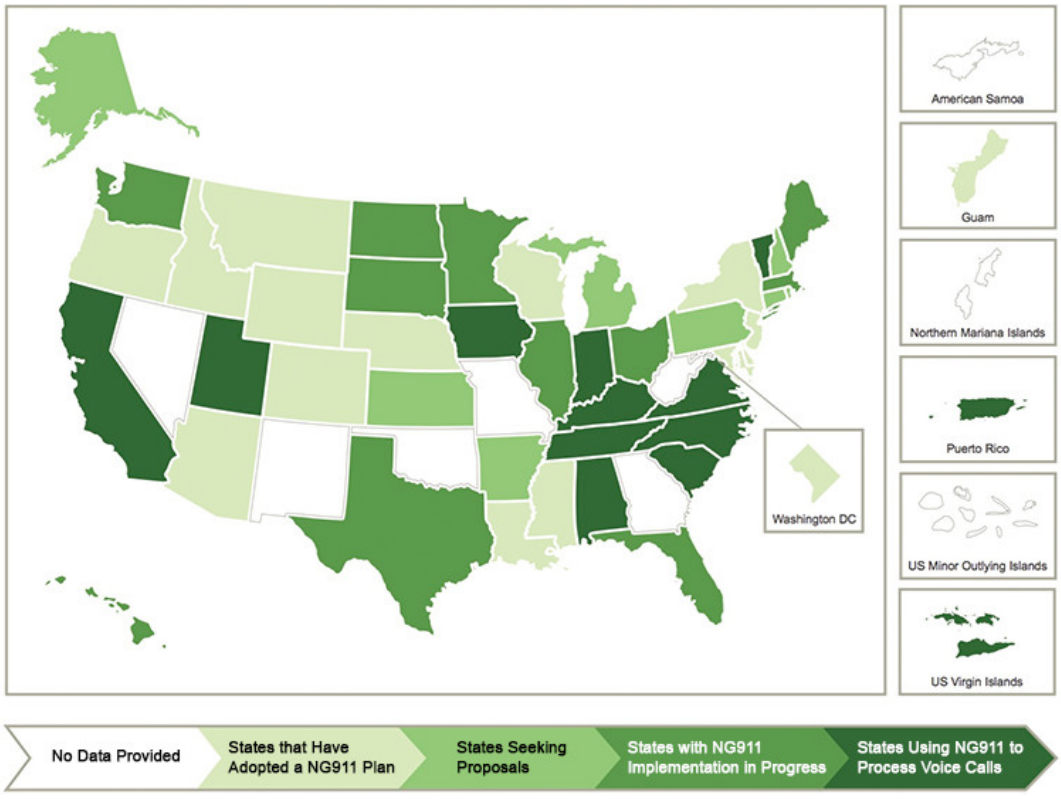
The pace of NG911 adoption by the states has rapidly increased since the program began collecting data, as shown in Figure 4-1. Moreover, when one compares the 2014 and 2017 state adoption maps in Figure 4-2 and Figure 4-3, respectively, the gap with Army mission partners becomes even more evident — many states with a significant Army presence are utilizing NG911 today. Given this rate of adoption, one would expect to see

even greater nationwide progress when the next report is released. It is important to note that much of the ESInet deployment has been paid with state government and/or federal grant funding — funds that DoD typically does not receive directly.



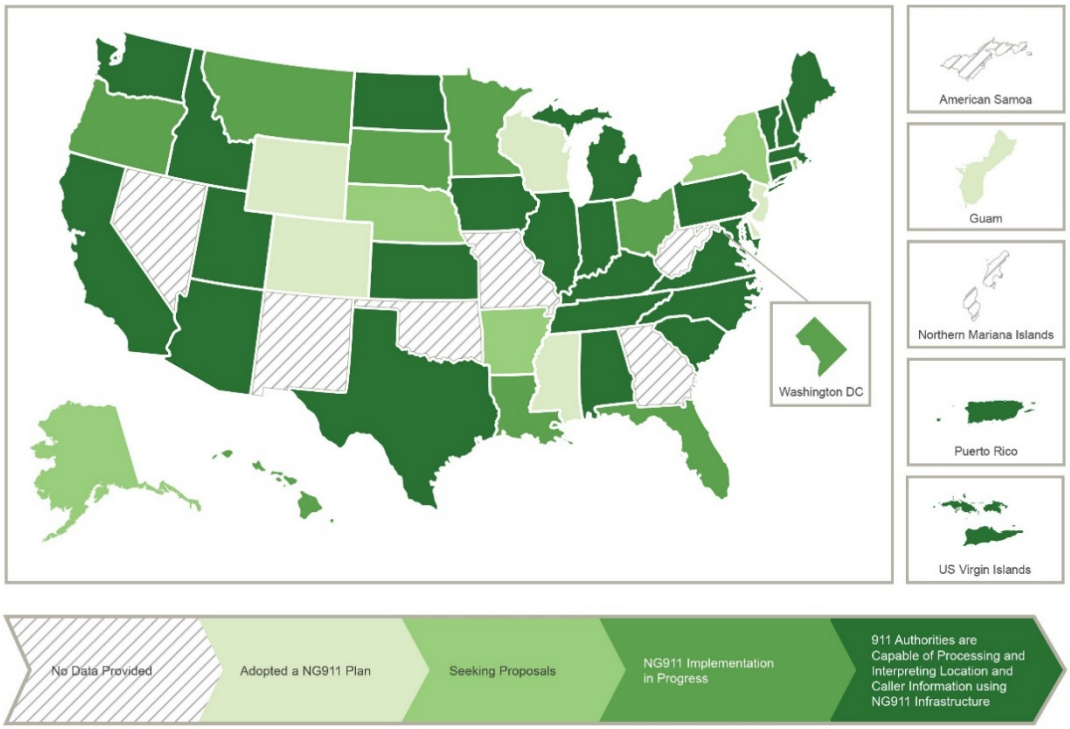
Note: Based on data contained in 911 Program Office report, *2017 National 911 Progress Report*.

Figure 4-1. State Deployments of NG911 2012-2017



Note: Reprinted from 911.gov, *2014 National 911 Progress Report*.

Figure 4-2. State's NG911 Progress as of 2014

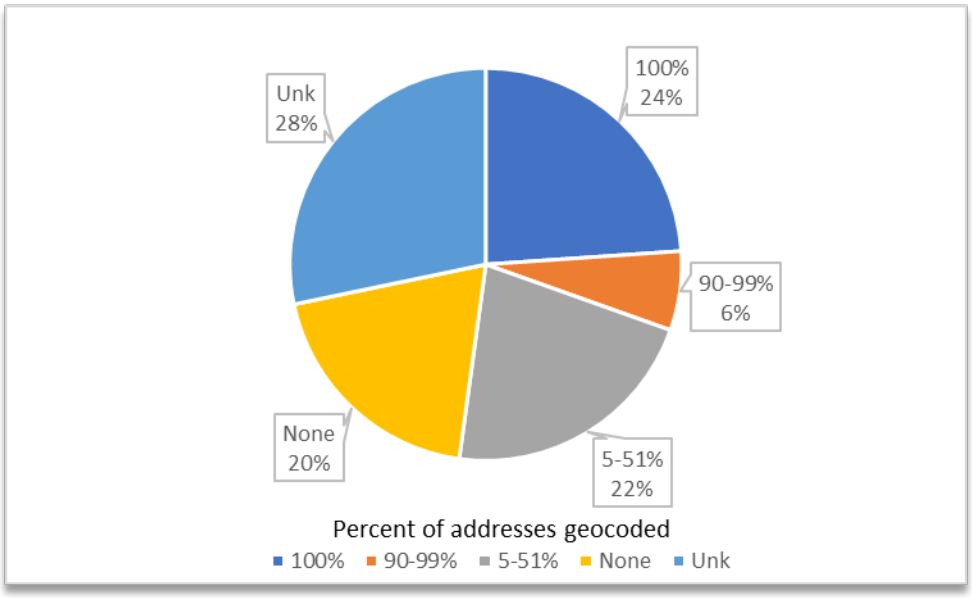


Note: Reprinted from 911.gov, *2017 National 911 Progress Report.*

Figure 4-3. States' NG911 Progress as of 2017

The 2017 study also examined states' progress on enhancing their GIS systems to an NG911-compliant format with *x* and *y* coordinates for each dispatchable address or location. As highlighted in Figure 4-4, nearly a quarter of all responding states reported that 100% of their addresses across the state had been geocoded, with another 6% of states reporting being 90% or more complete. Appendix B contains the state-by-state data.

Today, Army installations (as with most federal property) are black holes in the civilian first responders' maps. Until Army installations geocode their locations inside the fence, mutual aid partners will continue be hampered in responding to emergencies on a base. The Army GIS program under the Army Environmental Command within IMCOM is currently engaged in developing an enterprise approach to installation GIS supported by a local common installation picture developed at the garrison level. This work is critical in optimizing the Army's NG911 environment.



Note: Adapted from data contained in 911 Program Office report, *2017 National 911 Progress Report*.

Figure 4-4. States' GIS Geocoding Progress as of 2017

5. Migration Overview

Moving to a comprehensive NG911 environment entails more than replacing or upgrading the CHE and CAD systems to an all-IP environment. There are numerous additional integral components that combine to deliver an NG911 ecosystem that can replace the legacy analog ecosystem. Many of these components are outside the control of the Army. As such, an NG911 migration cannot be executed in a vacuum. The key considerations for the Army's migration plan include the timeline for the commercial carrier(s) serving installations to retire their analog infrastructure and the timeline of mission partners surrounding an installation to conduct their migrations. Ideally, the installation would migrate in coordination with those mission partners to avoid disruptions in mutual aid operations. As a last resort, legacy gateways can be used to provide some level of interoperability and information sharing, but this would be at a low level and would not deliver any of the benefits of NG911 to the installation.

To assist first responder agencies in their transition, the FCC chartered the Task Force on Optimal PSAP Architecture (TFOPA). The task force defined an implementation model with several phases so that PSAPs could follow a common methodology to align their efforts. The phases, as defined by the TFOPA, are as follows:[7]

Legacy State: *9-1-1 services are provided by the traditional incumbent local exchange carrier (ILEC) with circuit-switched infrastructure and Automatic Location Identification (ALI) circuits.*

Foundational State: *Groundwork and planning for NG9-1-1 implementation is initiated. NG9-1-1 feasibility studies are performed, Geographic Information System (GIS) data preparation commences, and IP networks may be implemented. NG9-1-1 systems are not yet operational and system procurement is either planned or underway.*

Transitional State: *Services have migrated partially from the legacy environment and the 9-1-1 services are enabled by an IP infrastructure. The Emergency Services IP Network (ESInet) is in place and Emergency Service Number (ESN) routing is still being utilized. This is the first state in which certain Next Generation Core Service elements may be implemented. At this point, a governance model has been established.*

[7] FCC TFOPA, *Working Group 2: Optimal Approach to NG91-1-1 Implementation, Final Supplemental Report,* December 2, 2016.

Intermediate State: *The 9-1-1 Authority has implemented and made operational all i3 Core functions within their control and all calls are routed per GIS boundaries and location information (i3 algorithms). Additionally, an i3 PSAP multimedia call handling system (terminating Emergency Services Routing Proxy (ESRP)) is implemented. Infrastructure and applications are being refined to incorporate advanced call- and data-delivery interfaces. Business and performance elements are maturing and are reviewed in regular intervals to optimize operations. Governance agreements are in place and the model is functioning. Systems in the Intermediate State are said to be NG9-1-1 READY.*

Jurisdictional End State: *PSAPs are served by i3 standards-based systems and/or elements, from ingress through multimedia "call" handling. Originating Service Providers are providing Session Initiation Protocol (SIP) interfaces and location information during call set-up time. Within the jurisdiction, ESInets are interconnected providing interoperability which is supported by established agreements, policies and procedures. Systems in the End State are NG9-1-1 Compliant.*

National End State: *PSAPs are served by i3 standards-based systems and/or elements, from ingress through multimedia "call" handling. Nationally, ESInets are interconnected providing interoperability which is supported by established agreements, policies and procedures. All systems in the End State are NG9-1-1 Compliant.*

By adopting this report, the Army takes the first step in the Foundational State of NG911 migration. Meanwhile, many of the Army's civilian mission partners have completed the Transitional and Intermediate stages, with the Jurisdictional End State phase in sight. Completing the Foundational State and working through the others will be a complex undertaking requiring alignment across the Army enterprise and with civilian mission partners. Adopting a comprehensive, strategic approach to an NG911 strategy and a phased implementation aligned with TFOPA guidance across the enterprise will facilitate meeting this goal and reaping the maximum benefits at the least cost.

A. Strategic Alignment

Achieving the to-be state is consistent with the following DoD and Army strategic documents and objectives outlined in Table 5-1.

Table 5-1. Strategic Alignment

Document	Goal/Objective (G/O)	Description
DoD Information Resources Management (IRM) Strategic Plan	G1/O2: Improve Information Sharing with External Mission Partners	The NG911 environment is natively capable of sharing information with mission partners through a shared ESInet or gateway
	G1/O4: Improve DoD's Information and Communications Technology (ICT) Support to Contingency Ops	Deployed troops in continental US (CONUS) Defense Support of Civil Authorities (DSCA) support operations will utilize equipment equivalent to that used by civilian authorities; equipment loaned by DoD during DSCA operations will integrate with existing civilian systems
	G2/O3: Enable Agile Decision Making through Mobile Applications	NG911 provides a rich, multi-media access to data from the initial call through the first responder's mobile devices for enhanced situational awareness and decision support
	G3/O2: Modernize Communications Systems/Leverage Commercial Technologies and Communications Capabilities	NG911 will migrate first responders off legacy 9-1-1 architecture to an IP-based one through adoption of ESInets
	G3/O6: Integrate Commercial Mobile IT Capabilities	NG911 provides a rich, multi-media access to data from the initial wireless call through to the first responder's commercial mobile devices
	G7/O2: Enable Information Sharing and Collaborative Agreements with Key Allies and Partners	Each installation has one or more key partners in the surrounding jurisdictions providing mutual aid, the NG911 environment innately enables information sharing
ANCP	O2.1: Increase the resiliency of the network defense posture by minimizing the attack surface	Adopting the NG911 standard and associated ESInet Border Control Function core service minimizes today's multiple attack

		vectors in first responder networks
ANCP Mid-term Implementation Guidance	Installation infrastructure modernization to improve wired information transport	The ESInet provides a robust and secure wired transport capability well beyond the capacity of the networks supporting first responders today
	Begin the transformation to a wireless infrastructure in Army installations	NG911 CAD natively supports end user devices on commercial mobile networks or private LMR
	Consolidate computing and storage infrastructure	The NG911 environment natively supports consolidation of PSAP infrastructure as in a “hub and spoke” model; NG911 also facilitates accessing cloud-based NG core services

6. High-Level Outcomes

The NG911 environment will deliver all the functional capabilities described in the to-be state of the *CAD Problem Statement* with the added benefits of migrating to the NG911 environment. This will ensure a secure, robust, and resilient system providing Army users with a best-of-class solution. Additionally, the new environment will be sustainable well into the future.

The pertinent high-level outcomes (HLOs) are listed below, with amplifying information provided in Tables 6-1 and 6-2:

- Comply with relevant standards, guidance, and accepted best practices:
    - FCC regulations
    - Department of Homeland Security
        - Emergency Communications Preparedness Center
        - Federal Emergency Management Agency
    - NENA
    - National Fire Protection Association
    - Association of Public Safety Communications Officials International

- Comply with relevant DoD and Army policies and guidance, including, but not limited to the following:
    - DoDI 6055.06, *DoD Fire and Emergency Services Program*
    - DoDI 6055.17, *DoD Emergency Management Program*
    - DoDI 8130.01, *Installation Geospatial Information and Services*
    - DoDI 8320.07, *Implementing the Sharing of Data, Information and Information Technology Services in the Department of Defense*
    - DoDI 8330.01, *Interoperability of Information Technology, Including National Security Systems*
    - 8500.01, *Cybersecurity*
    - DoDI 8540.01, *Cross Domain Policy*
    - CJCSM 3150.03D, *Joint Reporting Structure Event and Incident Reports*
    - USNORTHCOM Instruction 10-222, *Force Protection Mission and Antiterrorism Program*
    - AR 70-1, *Army Acquisition Policy*
    - AR 190-45, *Law Enforcement Reporting*
    - AR 25-400-2, *Army Records Information System*
    - AR 420-1, *Army Facilities Management*
    - AR 525-2 *The Army Protection Program*
    - AR 525-27, *Army Emergency Management Program*

- Provide enhanced capabilities for first responders, call takers, dispatchers, and emergency management personnel:
    - ESInet connectivity
    - NG Core Services
    - Integrated text-to-911
    - Deliver enhanced location information, including information from commercial cellular 9-1-1 calls placed from within the installation
    - Support multi-media information in the system end-to-end
    - Maintain “five nines” availability, i.e., 99.999%
    - Share information across the mission partner environment with DoD, federal, and civilian agencies
    - Interoperate with mission partners from DoD, federal and civilian agencies
- Provide the suite of HLOs defined in the *CAD Problem Statement* of 2015

Table 6-1. High-Level Outcomes

HLO Title	HLO Description
Interoperability	The NG911 system will have the capability to directly interface with legacy e911 as well as ESInets. The NG911 system will auto populate the supplied number and location data. The NG911 CAD system will directly interface with mobile date terminal (MDT) systems, the National Crime Information Center (NCIC), the Army Alert! system, and other needed databases. Army-owned and -operated NG911 components must meet Joint Interoperability Test Command (JITC) certification standards if deployed in the .mil environment. The NG911 system must also interact and communicate with outside NG911 systems in the communities around the installation on .gov networks. A common solution will facilitate the use of common information interfaces and standards, supporting more effective communications using existing command and control capabilities.
Communications	The NG911 environment will have multiple avenues and modes of communication with first responders, the public, open source information/social media, and outside first responder agencies and emergency organizations and databases.
Net-Readiness	The NG911 capability shall satisfy DoD policy concerning system interfaces and policy enforcement controls. This shall include an

	Enterprise or “Type” accreditation for Army-owned components in wide use at all installations, Certificate of Networthiness (CONs)//Approved Products List (APLs)/Department of Army (DA) and Local Configuration Control Board (CCBs). The NG911 capability will comply with the Joint Information Environment architecture, CIO/G-6 Cloud Computing Strategy and the Army Data Center Consolidation Plan. NG911 will be considered for cloud implementation. If local hosting is determined to be appropriate, then servers must be located in the approved Installation Processing Node, which may or may not be co-located with the Network Enterprise Center.
GIS	The NG911 capability shall integrate GIS data and mapping information while providing accurate real time locations of responder assets.
Human Systems Integration	The Provost Marshal Office (PMO) shall include user and administrative level training and a realistic drill scenario standardized across the Army. A first responder who transfers to another installation should be able to step into the new position and function successfully within the NG911 dispatch system. NG911 must have the capability to provide simulations to support initial and in-service standardized training requirements.
Maintainability	The NG911 capability shall allow routine maintenance and patching without significant deterioration of function. The system will be on a regular life cycle of quarterly upgrades and replacement.
Sustainability	The NG911 capability will be based on current standards avoiding obsolescence.

Table 6-2. HLOs and Measurement Criteria

HLO Title	Measurement	Current Baseline	Targeted Threshold	Targeted Objective	Benefits	Risks	Assumptions, Constraints, Dependencies
Interoperability	System info sharing across all emergency services and outside agencies. Linkage to all applicable military, local, state and Federal applicable databases	N/A	Interoperate with ESInet and LMR	Interoperate with Law Enforcement (LE) databases, Local first responders, and NG Core Services on NG911	Increased situational awareness across all installations and their Areas of Responsibility (AORs)	• Shortcomings in information sharing to first responders increase reaction times. • Lack of cooperation with local jurisdictions may hinder interoperability.	(A) Current CAD systems will not reach networthiness (C) Possible incompatibility with existing LE and first responder systems (D) HQDA and DoD providing Information Assurance (IA) policy oversight

HLO Title	Measurement	Current Baseline	Targeted Threshold	Targeted Objective	Benefits	Risks	Assumptions, Constraints, Dependencies
Communications	Wireless linkage with MDTs, LMRs, and modes of information sharing across all emergency services and outside agencies	N/A	Hardwire connections to ESInet, Installation voice, and LMR servers	Wireless connection to emergency communications systems and local and first responder assets	Increased situational awareness of asset distribution across the installation allowing for timely decisions	• Shortcomings in information sharing to first responders increase reaction times. • Delays in feedback from on-scene responders precipitates poor higher-level decisions.	(A) Legacy CAD and communication systems will continue to hinder reaction times (C) Possible incompatibility with all systems such as current land mobile net (C) Budget and financial costs
Net- Readiness	Accreditation across all installations	N/A	100%	100%	• Assured network services • Confidentiality, integrity and availability of Army data	• Compromised Army information systems. • Loss of data through security breach and exfiltration of sensitive data	(C) Budget and financial costs (C) Manpower at NECs (D) Interoperability

HLO Title	Measurement	Current Baseline	Targeted Threshold	Targeted Objective	Benefits	Risks	Assumptions, Constraints, Dependencies
Mapping	Highly accurate real time mapping of the incident location available end-to-end. Tracking of response assets.	N/A	100% real time incident and asset tracking at dispatch center	100% real time incident and asset tracking available to first responders	• Quicker response via instant routing. • Enhanced officer safety	Lack of real time asset data could lead to inaccurate situational awareness	(A) MDTs will have capability to receive this data (C) Budget and financial costs (C) Current installation GIS and mapping capabilities.
Human Systems Integration	First responders and dispatchers learn and implement program through in-person and simulation training	N/A	In-person training for new users	Training simulation embedded within NG911solution	Provides flexible training options with reference material	Reduced user proficiency and system effectiveness during transition to new system	(A) Training and Support Package (TSP) to include drilling will be included with cost of NG911 system (C) Budget and financial costs (C) Time to conduct training prior to fielding (D) System ease of interface (D) Availability of new users

HLO Title	Measurement	Current Baseline	Targeted Threshold	Targeted Objective	Benefits	Risks	Assumptions, Constraints, Dependencies
							due to work schedule
Availability	System up and running	N/A	99.999% system availability	99.999% system availability	Enhanced mission support		(D) Network infrastructure
Maintainability	System updates and maintenance scheduled periodically and conducted without taking the system down	N/A	Quarterly updates	Quarterly updates	Maintains system currency		(C) Budget and financial costs

7. Business Process Re-Engineering

The implementation of NG911 primarily relates to the service-to-satisfaction, end-to-end business process flow. An Army-enterprise NG911 capability will enable efficiencies, effectiveness, customer satisfaction, consistency, and reductions in operating costs for the delivery of emergency services on garrisons. Additionally, an enterprise approach will optimize the quality of service through the use of continuous performance improvement methodologies, leading to improvements of the Base Operations Support Requirements Model metric inputs. The NG911 environment will do the following:

- Facilitate predictable and consistent levels of service to soldiers, civilians and family members.
- Provide consistency to first responders as they are assigned to different installations.
- Enable greater productivity while demonstrating good stewardship of Army and taxpayer resources.

Table 7-1, Table 7-2, and Table 7-3 show the relationships between business outcomes and the Army's Business Enterprise Architecture and discuss metrics for measuring progress.

Table 7-1. Business Outcomes

HLO Title	Outcome	Definition
Interoperability	Achieve Army interoperability certification and Joint Interoperability Test Command (JTIC) certification	NG911 operates across a multi-agency, multi-jurisdictional environment across wireless and wired networks
Communications	Achieve ability to exchange multiple data types through various modes of wired and wireless communications	Communications linkage with first responders, the public, open source information/social media, outside LE and emergency organizations and databases
Net-Readiness	Achieve Risk Management Framework (RMF) Certification	RMF Certification achieves all Net-Readiness requirements
Mapping	• Geofile Synchronization • Location Validation • Asset Routing • Manual Location Entry • Topologically Integrated Geographic Encoding and Referencing (TIGER) files • Enhanced MSAG with *x*, *y* coordinates	• NG911 CHE and CAD systems shall support the creation and maintenance of a synchronized Geofile using an available mapping/GIS database • NG911 CHE and CAD systems shall verify incident location against the Geofile to determine its exact location • NG911 CAD system shall generate a route between asset locations and incident location • NG911 CHE and CAD systems shall support the ability to manually enter event location details. • Ability to map emergency response districts for police, fire and EMS using U.S. Census TIGER (like) shape and line data
Human Systems Integration	Training	The PMO shall include User and Administrative level training and a realistic drill scenario
Availability	System uptime of 99.999%	Enhanced mission support
Maintainability	Quarterly Updates	Maintains currency of system

Table 7-2. Business Outcomes and E2E Alignment

Business Outcome	E2E/BEA Perspective		
	Business Flow	**Business Process**	**Business Capability**
Achieve Army Interoperability Certification and Joint Interoperability Test Command (JITC) certification	Acquire-to-Retire	Concept-to-Product	Accredited Emergency Service across the force
Achieve ability to exchange data through various modes of communication (i.e., hardwired and wireless)	Acquire-to-Retire	Concept-to-Product Cost Management	Effective Communications
Achieve RMF Certification	Acquire-to-Retire	Concept-to-Product	Policies Match Usage
Geofile Synchronization Location Validation Asset Routing Manual Location Entry Topologically Integrated Geographic Encoding and Referencing (TIGER) files	Acquire-to-Retire	Concept-to-Product	Real time location services Mapping
Training	Acquire-to-Retire Market-to-Prospect	Hire to Retire Cost-Management	Program of Instruction (POI) in place
Maintain Data Availability	Acquire-to-Retire	Cost-Management	Secure in the Army Enterprise

Table 7-3. Business Outcomes and Measurement Criteria

Business Outcome	Measurement	Current Baseline	Targeted Threshold	Targeted Objective	Benefits	Risks	Assumptions, Constraints, Dependencies
Achieve Army Interoperability Certification and Joint Interoperability Test Command (JITC) certification.	• Standardized Army-Wide NG911 components. • Interoperability Certification	N/A	100%	100%	• Integrity and security of data at rest • Reduction in certification costs	• Disclosure of LE-sensitive, PII and HIPAA data • USACC goals are not met	(A)Single, standardized NG911 solution (C) Public Key Infrastructure (PKI) authentication enforced by system owners (D) PKI digital certificates
Achieve ability to exchange data through various modes of communication (i.e. hardwired and wireless).	• % of Infrastructure Communications (Hardwire connection to ESInet, NG core services, LMR servers and LTE services • % of Mobile Asset Communication (i.e., wireless connection to emergency communication	N/A	100% 100%	100% 100%	• Trusted business operations • Data exchange with multiple assets and systems	Compromised Army Information Systems	(A) Limits on communication with rapidly changing technology (C)Funding

Business Outcome	Measurement	Current Baseline	Targeted Threshold	Targeted Objective	Benefits	Risks	Assumptions, Constraints, Dependencies
	systems and local and first responder assets)						
Achieve RMF Certification	Standardized Army-Wide RMF certification	N/A	100%	100%	• Single certification process to operate on all Installations • Standard Implementation • Reduction in certification costs	Unknown RMF process flow and durations	(A) Single, standardized CAD solution
Geofile Synchronization	• % Delivery of real time incident and asset tracking at dispatch center • % Delivery of real time incident and asset tracking to local and first responders assets	N/A	100% 100%	100% 100%	• Faster response time • Increased situational awareness	Installation infrastructure (i.e., bandwidth limitations)	(A) Mapping data exists for Installation and local jurisdictions in a compatible format

Business Outcome	Measurement	Current Baseline	Targeted Threshold	Targeted Objective	Benefits	Risks	Assumptions, Constraints, Dependencies
Training	% of new users receiving training	N/A	100%	100%	Standardized training across all Installations	Installation staff availability and turnover	(A)Training provided by contracted vendor on a rotational basis during fielding with enough time to complete prior to implementation (C) One training event (multiple sessions) per Installation (D) Installation staff availability
System Availability	% of time system is available (up and running)	N/A	99.999%	99.999%	Enhanced mission support	N/A	(D) Network infrastructure
System Currency	Number of annual updates	N/A	4	4	System remains up-to-date		(A) Included in contract requirements

8. DOTMLPF-P Impacts, To-Be State

Table 8-1 summarizes how the NG911 solution impacts the DOTMLPF-P environment.

Table 8-1. DOTMLPF-P Impacts on "To-Be" State

Category	Impacts
Doctrine:	• NG911 systems are managed by Army NECs on approved networks and adhere to AR 70-1 and thus are part of the IA infrastructure with lifecycle replacement and upgrades • Single accreditation (if an enterprise solution is chosen) • Develop and implement common employment and sustainment doctrine for single technology, which will drive a common, standardized concept of operations
Organization:	• The 73+ affected installations belonging to IMCOM, MEDCOM, TRADOC and AMC are on a standardized NG911 solution that is managed cradle to grave • Single help desk service provided by the Army IT framework.
Training:	• Training is standardized and codified across all installations and can have employees trained within 2 weeks • Annual training requirements are outlined to maximize NG911 capabilities • Development and implementation of uniform training practices ensure improved performance across the inventory
Materiel:	• Common, standardized technical solution employed across Army Installations interoperable with response paradigm • IT hardware (i.e., computers and printers) and software are provided as part of each system and are standardized. Maintenance contracts are managed on the Army lifecycle management model, and systems are kept upgraded as new and evolving technologies improve efficiencies in the NG911 environment
Leadership and Education:	• Decisions regarding NG911 are made by Army Commands, Army Supporting Commands, and Direct Reporting Units and are standardized
Personnel:	• Position Descriptions are standardized across Army to allow uniform hiring • Qualified personnel are hired through the GS system or provided by contract support and are trained to operate the NG911 solution deployed to all installations. • Existing personnel will train and run the new NG9111 environment
Facilities:	• PSAPs have additional security concerns and restrictions and NG911 systems are separated physically but linked to the Army Enterprise and civilian mission partners as appropriate. • Existing structures can be used

Policy:	• NG911 will comply with information sharing policy DoDI 8320.07 • NG911 will comply with interoperability policy DoDI 8330.0 • NG911 will comply with cross-domain policy DoDI 8540.01 • NG911 will support AR 420-1, *Army Facilities Management*, for fire dispatch and response standard • NG911 will comply with IMCOM CLS standards. • NG911 will be acquired in compliance with AR 70-1, *Army Acquisition Policy*, using a system of systems approach that leverages aspects of the CIO/G-6 and ASA (ALT) Common Operating Environment (COE) Architecture and the DOD IT Strategy Roadmap • NG911 will comply with AR 525-2, *The Army Protection Progra*m

9. Alternative Deployment Models

The NG911 architecture, evolving best practices such as regional PSAP consolidation, and new cloud-based commercial offerings have enabled alternative ways of deploying NG911 with significant impacts on cost as well as business practices. These alternatives did not exist or were not feasible in the legacy 911 environment. Each model comes with its advantages and challenges, as summarized in Table 9-1, and each should be examined in greater detail in an AoA as part of a larger BCA effort. Briefly, each alternative can be defined as:

Traditional: A traditional approach utilizes standard government acquisition approaches and vehicles. The result is a solution that is wholly acquired, deployed, and maintained by the Army. All systems would reside on .mil networks and be subject to CAC authentication, JTIC accreditation, and all other DoD and Army policy requirements.

Hybrid: A hybrid model entails leveraging the mission partner environment by utilizing some or all of an NG911 solution deployed by one or more civilian jurisdictions abutting an installation. Given the relatively low call volume on an installation compared to a civilian PSAP, scalability of the solution is unlikely to be a barrier.

Examples of hybrid models include Joint Base Charleston and Charleston County, South Carolina (Appendix D) and Fort Carson with El Paso and Teller Counties in Colorado (Appendix E). Other jurisdictions with a large military presence are proactively planning for potential DoD users on their NG911 systems, as seen in the RFP recently released for the Virginia Beach, Virginia regional ESInet (Appendix F).

As-A-Service: Recent commercial offerings allow acquiring NG911, in whole or in part, as a service. One could acquire CHE as a service or a complete end-to-end solution. In this model, the solution is delivered via a web interface with little or no vendor equipment being installed in the .mil environment. At least one civilian PSAP with a significant military presence in the region has piloted this model.

Table 9-1. Deployment Alternatives

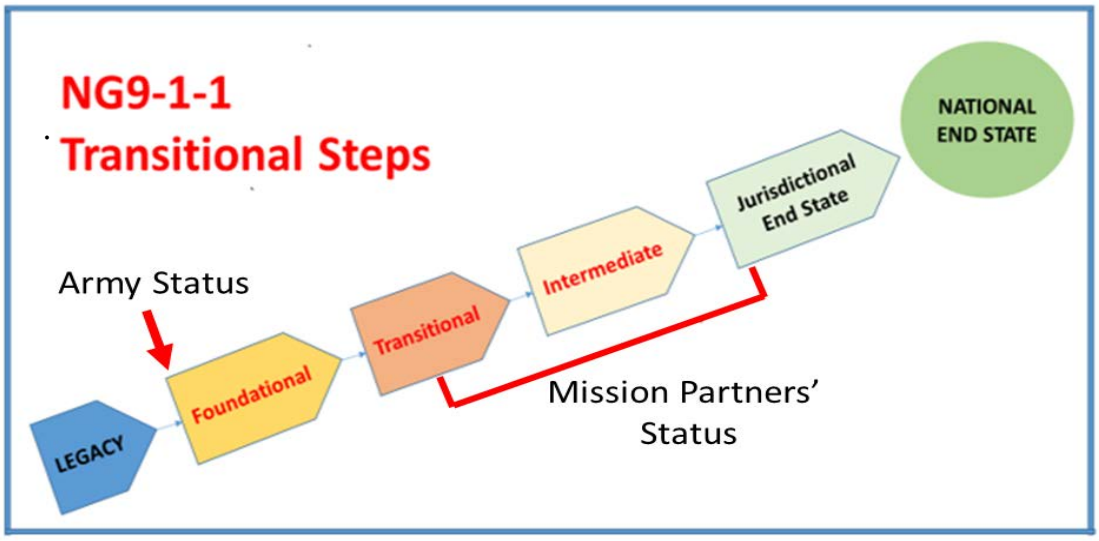
Model	Description	Advantages	Challenges
Traditional	100% Army-acquired, deployed and operated solution	• End-to-end control of the solution • Standardized PSAP environment across the enterprise	• High cost • Complicates mission partner environment • Cross-domain security required • Accreditation and certification processes
Hybrid	Participate in NG911 solutions deployed by local civilian mission partners	• Leverage federal and state funding • Avoid cost of building ESInet • Enhanced mission partner environment • Existing models for reference	• Changes in business processes • Non-standard PSAP solutions across the enterprise
As-a-Service	Subscription-based cloud solution	• Low cost • Installation can focus on core competencies • Integration with mission partner • Easy to deploy	• Changes in business processes • Cede some level of flexibility

10. Summary and Recommendations

Today's as-is technical environment supporting emergency call processing and first responders represents a clear and growing capability gap with the Army's civilian mission partners. This gap constrains mutual aid operations and directly increases the level of risk to life and property on Army installations.

Civilian mission partners across the Unites States, as well in some locations outside the CONUS, have already made substantial progress in their migration from the legacy environment to NG911. The Army must also make this migration to close the capability gap. As highlighted in Figure 10-1, this gap can range from moderate to severe, depending on location, when measured against the TFOPA transition model.

With the currently installed, analog-based technologies at end-of-life, the migration must also be made to ensure that any capability at all exists when the commercial providers retire their legacy network equipment. A failure to migrate to NG911 will eventually lead to loss of all standards-based emergency call processing capability and an increased level of risk.



Note: Adapted from a graphic in TFOPA Working Group 2, *Final Supplemental Report*, December 2, 2016.

Figure 10-1. NG911 Transition Status

The recommendations in Table 10-1 focus on near-term actions required to complete the Foundational State and move into the Transitional State. The strategy and migration planning entailed in these recommendations will guide further actions for attaining the Intermediate and End States.

Table 10-1. Recommendations

Recommendation	Discussion
Recommendation #1: ***Implement a governance body***	An overarching governance body and structure is needed to provide oversight and guidance for all activities involved in the transition. The governance scope should be enterprise-wide. As NG911 is a cross-cutting capability, stakeholders from all beneficiaries of the new environment should be represented on the governance body.
Recommendation #2: ***Develop an enterprise NG911 strategy.***	A high-level NG911 migration strategy detailing specific goals and objectives should be developed by the governance body. The strategy should contain a policy analysis to identify any potential DoD or Army policy constraints that would require mitigation to facilitate deploying NG911.
Recommendation #3: ***Conduct a business case analysis (BCA)***	A detailed BCA utilizing the DoD BCA template should be conducted. The analysis of alternatives in the BCA should include traditional, hybrid, and NG911 as-a-service options with estimated procurement costs for each.
Recommendation #4: ***Complete GIS enhancements***	The ongoing GIS enhancements should ensure that all locations of interest, addresses, building identifiers, etc., are fully geocoded with *x* and *y* coordinates. Installation-level GIS should follow NENA i3 guidelines to maximally support NG911. GIS data at the For Official Use Only (FOUO) level and below should be integrated with the shared next-generation mapping services of the surrounding jurisdictions.
Recommendation #5: ***Develop and execute a deployment strategy***	Based on the results of the BCA, a deployment strategy, including the acquisition of the solution, can be developed and executed. Memorandums of Understanding (MOUs) and other agreements with civilian agencies would also need to be executed if required. This is the last requirement to exit the Foundational State and enter the Intermediate State.

Appendix A.
States' NG911 Status

Table A-1. NG911 Status for States with Major Army Installations

State	Status	# PSAPS on ESInet	Installations
AL	Statewide contract in place	118	Fort Rucker, Redstone Arsenal
AK	N/A		
AZ	Maricopa region planning effort	6	Fort Huachuca, Yuma Garrison
AR	N/A		
CA	Statewide contract in place	37	Fort Hunter Liggett, Fort Irwin, Presidio of Monterey
CO	Working group in place		Fort Carson
DC	Statewide contract in place		
FL	Plan in development		
GA	N/A		Fort Benning, Fort Gordon, Fort McPherson, Fort Stewart
HI	N/A	6	
IL	Statewide transition targeted for 2020	19	Rock Island Arsenal
KS	Statewide contract in place	47	Fort Leavenworth, Fort Riley
KY	State plan adopted	20	Fort Know, Fort Campbell
LA	N/A	1	Fort Polk
MD	Fiber connectivity for an ESInet in most primary PSAPs.		Aberdeen Proving Ground, Fort Detrick, Fort George G Meade
MA	Statewide contract in place	40	
MI	Legislation introduced	61	Detroit Arsenal,
MO	N/A		Fort Leonard Wood
NJ	N/A		Fort Dix, Picatinny Garrison
NM	N/A		White Sands
NY	Working group in place		Fort Drum, Fort Hamilton, West Point
NC	RFP released, have not selected a vendor at this time		Fort Bragg
OK	N/A		Fort Sill
OR	Transition strategy adopted		
PA	Statewide plan adopted	24	Carlisle Barracks

PR	Statewide contract in place		Fort Buchanan
SC	Implementation plan in place		Fort Jackson
TX	Statewide contract in place	303	Fort Bliss, Fort Hood, Fort Sam Houston
UT	Statewide contract in place	12	Dugway Proving Ground
VA	Statewide contract in place		Fort A P Hill, Fort Belvoir, Fort Eustis, Fort Lee, Fort Monroe, JB Myer-Henderson Hall
WA	Statewide contract in place	54	JB Lewis-McChord
WI			Fort McCoy
WS	Contract in place for some NG911 components		

Source for state data: 911 Program Office, *2017 National 911 Progress Report*.

Appendix B.
States' NG911 GIS Status

Table B-1. Percentage of Addresses Geocoded for NG911

State	%	State	%
AK	7	MN	60
AZ	50	ND	50
CT	100	OR	100
DC	100	SC	95
HI	100	SD	97
IA	87	TN	100
ID	50	TX	13
IN	100	UT	100
KS	98	VA	100
MA	100	VT	100
ME	100	WA	83
MI	39	WY	40

None: AR, CA, MT, MC, NE, NM, PA, PR

Unknown: AL, CO, FL, GA, IL, KY, LA, MD, OH, OK, VI, WI

Not reported: AS, DE, GU, MO, MS, NH, NV, NY, RI, WV

Source: 911 Program Office, *2017 National 911 Progress Report*.

Appendix C.
CAD Problem Statement
Version 3.3 18 June 2015

Department of the Army

Computer Aided Dispatch (CAD) Capability

Problem Statement

Version 3.3
18 JUN 2015

Based on Business Case Template Version 1.0, August 2014

Document Revision History

Version	Date	Summary of Changes
Problem Statement Version 3.0	18 November 2014	IMCOM changes integrated
Problem Statement Version 3.1	08 January 2015	ROM Added
Problem Statement Version 3.2	20 May 2015	BPR updated (3.2.2), Problem Scope updated (Page 3)
Problem Statement Version 3.3	18 JUN 15	Adjudication

Table of Contents

Problem Statement Signature

Functional Sponsor: ***Date:***

Director, OBT

Problem Statement Approval

IRB Chair: ***Date:***

<Insert name here>
<Insert title here>
<Insert organization here>

Section 1. Executive Summary

Problem Statement

Various locally procured Computer Aided Dispatch (CAD) systems are being used on Army installations posing cybersecurity risks and are not in compliance with Army Regulation (AR) 70-1, Army Acquisition Policy, as some systems are not accredited and are vulnerable to cyber threats. As a result, the Army has not complied with the System of Systems approach and installations experience fluctuations in the quality of emergency services from installation to installation. CAD systems on Army installations do not fully integrate with Enhanced 911 and other emergency services. Many do not have the capability to digitally communicate reports of incidents, location, situational information, and background information by interfacing with authoritative informational data sources and providing enterprise level situational awareness/information sharing to assist military and civilian law enforcement, fire and medical. This causes delays in dispatch and response times, increased risk to property and personnel, and resource management constraints. The desired CAD capability will provide secure and reliable digital communications to assist military and civilian emergency personnel with emergency management operations

Problem Description

CAD is a central hub capable of dispatching law enforcement/fire/medical services. Currently, installations across the Army are using various, locally procured CAD systems to meet Installation Management Command (IMCOM) Common Level of Service (CLS) requirements for dispatching and response. In many instances, Installation Provost Marshal Offices/Directorates of Emergency Services (PMO/DES) are employing non-standard equipment with closed architecture and proprietary solutions. CAD systems had historically been procured using Operations & Maintenance (OMA) funds because it was the only available funding to the installations, however the enterprise solution requires Research, Development, Test & Evaluation (RDT&E) and Other Procurement Army (OPA) funds.

Problem Scope

In calendar year 2013, IMCOM tracked 31 Continental United States (CONUS) installations with various forms of (non-standardized) CAD. The Office of the Provost Marshal General (OPMG) conducted an analysis in 2014 using the IMCOM CY 13 CLS which reflected installation output measures as it related to CAD, Enhanced 911, and 911, in addition to CAD Year Lifecycle, Annual Maintenance Cost, whether the CAD was on the .mil Domain and if the CAD could communicate with responders using wireless. Currently, 41 of 72 Army Installations do not have an existing CAD capability and 12 suppliers provide disparate capabilities to 31 Installations. An investment needs to be made to establish an Army baseline.

The analysis further reflects significant improvements in the areas of enterprise digital information sharing, and connectivity between emergency dispatching systems and first responders for those installations with a CAD capability, especially with civilian mutual aid for Fire Response. First responders require approved Mobile Data Terminals (MDTs) that interface with other protection related security and emergency services information capabilities. These terminals must be NIPR/LandWarNet capable, with approved certificates of networthiness. Unless the Army approves procurement of enterprise level CAD capability, PMO/DES will not have an integrated ability to digitally receive, distribute and/or track incident responses and calls for emergency services.

Results clearly articulated that all installations with appropriate dispatch resources reported “Green” (rather than amber, black or red) in CLS output measures for Law Enforcement Response times when the installation was equipped with a CAD system that integrated with an Enhanced 911 system. CLS Output measures clearly measure the “Emergency Response Times” for law enforcement first responders. A full service CAD enables the Dispatch Operations to instantly locate the nearest unit to the emergency for

improved dispatch and response times during emergencies. Even when first responders were not fully staffed, a CAD system enables Emergency Services to respond to a critical emergency with the nearest unit saving critical minutes in response and dispatch times. Results also proved that Enhanced 911 capability is maximized when integrated with CAD. Results of annual maintenance cost are $1,027,541 per year. This does not include a $120k DoD Risk Management Framework (RMF) certification (previously known as Information Assurance Certification and Accreditation Process (DIACAP)) per year for each CAD. The cost varies across installations based on the type and complexity of the CAD, the cost ranges from $300 to $200k. The CLS standards do not improve based on maintenance cost; some of the most expensive CAD maintenance contracts are in the RED on their dispatch or response based on connectivity issues. CAD maintenance can be reduced by having one system contract that is maintained centrally at a reduced cost. In addition, the RMF cost would be for one enterprise system not 31 separate systems that all need accreditation.

Results on the impact of the CAD being on the .mil Domain were not significant enough to draw any correlation with dispatch or response services. However, there was a correlation with whether the CAD can communicate with responders using wireless with a reduction in timeliness of dispatch and response services. This is attributed to the CAD not communicating with the Mobile Data Terminals (MDTs) in the responder's police vehicles and not being able to timely transmit information wireless versus over the radio which slows the information flow.

Problem Solution

In accordance with AR 70-1, the CAD capability must use a System of Systems approach that leverages aspects of the Chief Information Officer (CIO)/G-6, Assistant Secretary of the Army for Acquisition, Logistics and Technology (ASA (ALT)), Common Operating Environment (COE) Architecture and the DOD IT Strategy Roadmap. This will allow for a standardized, scalable and common technical solution across diverse Installation sizes with the ability to integrate and interoperate with emergency response capabilities. OPMG requests appointment of an ASA (ALT) office to oversee the provision of CAD.

Recommended Course of Action

The recommended course of action is to assign a Program Executive Office (PEO) to conduct analysis to determine the most fiscally efficient and effective CAD available to meet Army's enterprise requirements and industry standards from The Law Enforcement Information Technology Standards Council and many variants of Commercial Off The Shelf (COTS) CAD systems.

Upon completion of PEO designation, appropriate CAD system selection and installation prioritization, the Program Manager (PM) should provide OPMG with a Memorandum of Notification that includes the intent to field the capability to each installation (physical or virtual enterprise deployment) within each fiscal year. At a minimum, the following products for each selected installation/facility will be provided:

(a) Materiel Fielding Plan, that includes timelines, coincides with installation/facility blackout dates and the Total Package Fielding concept, as necessary.

(b) Materiel Requirements List, (as applicable) will include Item Unique Identification tags utilized by the Installation Property Book Officer.

(c) Materiel Fielding Team Requirements will clearly identify the scope of assistance from the gaining command and what they will provide to the command to ensure an efficient and effective fielding operation.

(d) Modeling and Simulation will be utilized by the PM to help establish the "to be" capability of installations of different size variants (major, large, medium, small) as related to the capability gaps being addressed.

During post fielding and sustainment, per AR 700-127, Integrated Logistics Support, the PM provides the Army and each installation a life cycle sustainment plan (LCSP) planning document that reflects a post-fielding support plan, which will carry all materiel and software through a minimum of three-year program sustainment (vendor warranty or Government off the shelf (GOTS) sustainment). This LCSP will include sustainment life cycle costs, as the Service will be responsible for sustainment throughout the materiel's life cycle (cradle to grave). The PM then ensures a viable sustainment transition plan, between the program and the Service, is incorporated to ensure proper Total Cycle Life Systems Management and Performance Based Logistics. The Life Cycle Manager in turn participates in a continuous refreshment program to acquire an improved System of Systems to include obsolescence management oversight.

The PM provides installation owning commands (e.g. IMCOM) with a plan for maintaining software sustainment, configuration and version control for all command and control and computers. The design, development, purchase and installation of CAD systems involves not only the installation of computers (as well as mobile computers or smart devices) and the CAD software, but usually is connected to a wide variety of other systems: alarm inputs, mobile data systems, time synchronization sources, dispatch protocols, records management systems, CAD systems of other agencies, and the local, county, state and federal network of criminal justice databases.

This initiative supports the Army Campaign Plan and major objectives: 2.1 Deliver Services that Support the Total Force and Protect Installations, People and The Environment, 5.2 Equip and Modernize the Army, 5.3 Maintain a Leading Edge in Technology, 9.0 Sustain and Enhance Business Operations and 9.1 Improve Business Processes.

It also supports IMCOM lines of effort (LOE) 2: Effective Base Operations Support Services and LOE 3: Infrastructure sustainment and revitalization. These Command efforts support IMCOM's top Priorities 2: Posture the Command to support Army Priorities and IMCOM's Vision for the future and 5: Transform IMCOM Garrisons to support and enable Army Force 2025.

Rough Order of Magnitude:

Rough Order Estimate of the cost to implement Armywide CAD application is approximately $487.2 MIL over 15 years.

$487.2M 15-Year Lifecycle = $208.6M Implementation (Y1-Y3), $278.6M sustainment (Y4-Y15)

Benefit:

A standardized CAD system procured and implemented on an enterprise level will reduce the loss of life and property, increase situational awareness and improve reporting and analysis of incidents. CAD systems reduce the loss of life and property by automating incident creation and minimizing dispatch and response times as identified in the Fort Hood Army Internal Review. The system also improves situational awareness by sharing information from authoritative data sources (i.e. communications systems, law enforcement databases, etc.) with military and civilian first responders. Pre-programed CAD protocols improve efficiencies by reducing dispatch times and reducing first responder response times to all emergency situations. Additionally, CAD allows for real time asset management, tracking the location and status of individual assets (personnel and equipment) which provides a superior real time common operating picture throughout the entire incident lifecycle. This data can be used during or after the incident, providing forensics of key performance indicators. Furthermore this data improves future manpower modeling based on calls for service tracked within the CAD system. The monetary return on investment is based on a scalable solution that takes into consideration the size and scope of the installation mission set, this will provide a cost effective strategy.

Using a System of Systems (SoS) approach through the enterprise solution with a Program Management Office, will provide a centralized life-cycle management for the CAD program that streamlines cost, schedule and performance, while minimizing risk with cyber security management. Exploiting existing Commercial off the Shelf systems it provides opportunities to reduce life-cycle costs by garnering economies of scale, centralizing configuration and ensuring system integration and interoperability.

The Economic Viability Tool (EVT) did not take into account that each installation costs are flexible and not every installation will not need the same resources based on their mission needs. The EVT also does not correlate to the value of lives saved, reduced response time to critical emergency situations and performing life saving measures. Government agencies have documented the Value of Statistical Human Life (VSL), to include the Environmental Protection Agency, the Office of Management and Budget (OMB), and Harvard Law School. Using the lowest cost estimate from OMB at $6.4M each, a deduction can be made that if the enterprise CAD reduces response time and raises the survival rate by at least 20% the total investment of CAD will save around $33M to the Army.

Value of statistical life:

a. VSL (OMB) = $6.4M each
b. Average number of traffic fatalities per calendar year = 27, multiplied by VSL $6.4M = $172.8M
c. $172.8M x 15 year lifecycle of the program = **$2.6 Billion in Total Cost of Life**

CAD Estimated ROM Costs:

a. Total ROM for CAD over 15 years = $487M
b. Total cost of CAD investment equals 18% of total loss of life

CAD reduces response times:

a. Studies indicate that reduced response times raise survival rate by at least 20%
b. 20% of $2.6B = $520M VSL savings.

OMB VSL Rate = $33M dollars over the (15year) life of the program ($520M saved life - $487M total cost of investment = $33M savings).

Section 2. Introduction

2.1. Purpose

The purpose of this document is to establish a business case for Defense Business Council (DBC) approval of an Army enterprise capability for Computer Aided Dispatch (CAD) to conduct daily emergency management operations on Army installations. The goal is to integrate as many functions and workflows as possible across emergency management functions to reduce costs and improve efficiency and effectiveness.

2.2. Background

The OPMG is responsible for policy, plans, programming, and oversight of law enforcement services on Army installations. OPMG plans to establish a requirement for a CAD capability in support of the emergency management mission. An Army enterprise CAD capability requires the identification and implementation of a secure, accessible, integrated, and standardized CAD information system to conduct daily emergency management operations.

The 2009 Army Internal Fort Hood Report's findings directed modernization of emergency management and first responder capabilities. The Fort Hood Report describes the ability to quickly and efficiently dispatch law enforcement and other emergency service assets is a critical part of protecting personnel and property on any Military Installation. The standards for CAD systems are established by The Law Enforcement Information Technology Standards Council (LEITSC). Created in 2002, it brings together

representatives from the International Association of Chiefs of Police, National Sheriffs' Association, National Organization of Black Law Enforcement Executives, and Police Executive Research Forum to address law enforcement information technology standards issues. LEITSC has published Standard Functional Specifications for Law Enforcement CAD Systems. The CAD functional specifications provides a starting point for law enforcement agencies to use with developing CAD requests for proposal, level the playing field when working with vendors, and promote system interoperability. This is especially vital for coordination and response involving off post agencies.

CAD is a technical software/hardware system which assists dispatchers, call-takers, and 911 operators in tracking, monitoring and rapid dispatching of first responders using geographic information system (GIS) mobile technology, pre-programmed protocols getting the nearest responders quickest to critical incidents, while maintaining records of these responses. CAD is a system used by dispatchers and first responders to log, track, dispatch and assign calls for service. A CAD system manages information from many other responder systems to optimize the dispatch of responder personnel. The size and complexity of the CAD system are determined by the needs and requirements of the agency and the existing systems that the agency would like to integrate. CAD implementation involves installation of servers, computers, and software, as well as connection to a variety of other existing systems. CAD systems are usually located in a central dispatch office or public safety answering point. With the support of dispatchers, CAD servers communicate with call center computers/phones, cell phones, MDTs installed in vehicles, two - way radios, and fax servers. This provides dispatchers and field personnel multiple communication options. CAD systems may also interface with an automatic vehicle location (AVL) system, a caller identification (ID) system and logging recorders.

The majority of CAD systems can incorporate information from the following systems: records management systems (RMSs), GIS, AVL, and caller ID. RMS provides data relevant to the current service call. GIS provides numerous types of geographical and geospatial data; AVL pinpoints the location of response vehicles, which allows the CAD system to help determine the most suitable unit for response; and caller ID verifies the exact location of an incoming call and/or incident.

CAD systems allow public safety operations and communications to be augmented, assisted, or partially controlled by an automated system. It can include, among other capabilities, computer-controlled emergency vehicle dispatching, vehicle status, incident reporting, and management information. All aspects of a CAD system must be optimized for rapid response time and system reliability. Since time is of the essence, the CAD system must accurately provide a data and time stamp for every activity. CAD systems collect the initial information for an incident and then provide the information to one or more records management systems. The CAD system also supports other activities that assist in the effective use of public safety resources, including shift change roll call, "Be on the lookout" (BOLO) files, and the ability to schedule a call in the future.

The design, development, purchases and installation of CAD capabilities involves the installation of computers (mobile computers or smart devices) and the CAD software. It also involves connectivity to other systems: such as alarms, duress devices, and records management systems. Due to mutual aid requirements of Army fire and medical emergency services between local and or other DoD agencies, Army CAD capabilities must include interfacing with the local, county, state and federal dispatching and public service answering points.

CAD systems are most commonly installed by the vendor with the assistance of agency employees who are familiar with the agency's infrastructure, network, and systems' configuration. The complexity of the CAD system and the level of integration with existing systems determines the time required for installation.

Maintaining a CAD system usually requires a trained systems administrator and a CAD administrator. The systems administrator is typically responsible for maintaining the network, servers, databases, and software patches at an agency. Responsibilities of the CAD administrator may include maintaining the response plans, incident types, and paging configurations in the CAD system. Warranties will vary by vendor, and many offer ongoing maintenance and/or technical support options.

Section 3.

3.1. "As-Is" Analysis

3.1.1. The Problem

CAD capabilities are currently employed in a fragmented operational, training and sustainment environment and are managed at the individual installation level. CONUS and Outside the Continental US (OCONUS) installations have historically procured non-standard equipment with closed architecture and proprietary software with OMA not OPA funds. Table~~Figure~~ 1, drills down the CLS dispatch standards by installation and includes their lifecycle expiration date and their rate of workload as depicted by the number of completed police reports. 31 out of the 39 IMCOM installations have a CAD system. Using the IMCOM CLS reflected that current installation output measures as it relates to CAD, e911, and 911, revealed that 14 of the 31 IMCOM installations reported the best performance to IMCOM when the installations had both CAD and some form of enhanced 911 working together as a complete system. However, the analysis also reflected that 18 of the 31 (58%) installations' maintenance support for CAD has either expired or will expire within this Fiscal Year. The major results were:

- Current CAD capabilities are not standardized
- Not interoperable or integrated solutions (i.e. does not share information with E911 systems, does not talk to first responder vehicles in approved accredited fashion)
- Installations have varying levels of CAD capability (some with no CAD capability)

	E911+CAD	911+CAD	E911	911	CAD	Neither	CAD Year Lifecycle	Total Police Reports for CY 13
Fort Bragg							2016	High
Joint Base Lewis McCord							2013	High
Fort Polk							2013	High
Fort Stewart							2013	Medium
Fort Drum							2014	High
Fort Carson								High
Fort Jackson							2013	Medium
Presideo of Monterey							2017	Medium
Fort Irwin							2015	Medium
Fort Sill							2014	Medium
Fort Gordon							2013	Medium

Fort Huachuca							2013	Low
Fort Wainwright							2013	Low
ROCK ISLAND ARSENAL								Low
USAG Humphreys							2014	Medium
Aberdeen Proving Ground							2013	Low
Fort Rucker								Medium
Redstone Arsenal								Medium
Fort Greely								Low
Fort Lee								Low
Picatinny Arsenal								Low
Detroit Arsenal								Low
Joint Base Myer-Henderson Hall							2015	Medium
Carlisle Barracks								Low
Fort Campbell							2012	High
Fort Knox							2016	High
Fort Benning							2017	High
Fort Riley							2016	High
Fort A.P. Hill								Low
Fort McCoy							2016	Medium
Fort Leavenworth								Low
West Point (PMO)								Medium
Dugway Proving Ground							N/A	Medium
USAG Hawaii								High
Fort Bliss							2014	High
White Sands Missile Range							2005	Low
Fort Hood								High
Fort Leonard Wood								Medium
Fort Belvoir							2013	Medium
Fort Meade							2015	Low

Table 1

Color = Capability Level (# of calls for emergency dispatch, # of alarm activations, #of NCIC/VERINET queries)

Green = Achieves full mission capability with immediate and competent response to 100% of emergency calls 24/7; Immediate and competent response to 100% of alarm activations 24/7; Immediate initiation of action to dispatch units 24/7; Timely response for patrol

Amber = Expected degraded mission capabilities. Some calls/patrol queries may not be answered/dispatched timely if the dispatcher is engaged with one or more calls

Red = Serious degradation of mission capabilities. Several calls/patrol queries may not be further delayed if the dispatcher is engaged with one or more calls.

Black = No capability

Total Police Reports:

High = > 3,000
Medium = > 1,000, <3,000
Low = < 1,000

3.1.2. Problem Description and Context

An analysis of these systems reflect shortcomings in the areas of enterprise digital information sharing, and connectivity between emergency dispatching systems and first responders' abilities to receive information and directives to respond to incidents and emergencies. First responders require approved MDTs that interface with other protection related security and emergency services information capabilities. These terminals, if attached to NIPR/LandWarNet, the MDT must have a certificate of networthiness. Unless the Army approves the procurement of an enterprise level CAD capability, PMO/DES will not have an integrated ability to digitally receive, distribute, and track incident responses and emergency service calls.

To eliminate current functionality gaps and to address new law enforcement requirements a new system is needed that will automate core law enforcement business processes and will result in a more standardized, integrated, and efficient Army enterprise information technology solution. A CAD system must provide a level of scalability and compatibility with other law enforcement and emergency management systems and be in compliance national and DoD standards and specifications.

It is the intent of OPMG to adapt to current industry best practices as it relates to the emergency response operating procedures and the operating environment of CAD. Implementing CAD will enable key stakeholders the opportunity to assess current operating procedures against any productivity gains that can be realized through the introduction of automation.

3.1.3. Root Cause Analysis

The current usage of non-standardized CAD systems causes a number of problems in addition to lack of connectivity to the Army enterprise.

First, the widest variety of communication and geo locating options such as call center computers/phones, cell phones, mobile data terminals (MDT)s installed in vehicles, two -way radios, and fax servers are not uniformly provided between installations. As non-standardized CAD systems have aged, connectivity to changing communication options have not been maintained across the force. The ability to know the location of first responders and their proximity to risks and hazards in real time while in constant

communication with these assets is imperative. Communicating accurate information will enhance the safety of first responders and the public. By providing real-time information from the scene, it allows senior stakeholders to make better decisions on asset deployments, which would enhance the protection of the public and property.

Second, many of these systems are not compatible with the counterpart civilian systems used in the communities around our military installations. These systems were different priority from place to place and constrained by varying budgets. This caused installations to lag in upgrading systems on a regular basis while their civilian counterparts continued to improve and keep up with current technologies. This same constraint has kept systems from keeping pace with Army life cycle systems. Non standardized CAD systems in turn cannot be added to the network or simply upgraded. They may also lack the ability to provide simulation tools to support training and exercises in incident response.

Third, many of these new technologies have changed the way civilian police operate and improved efficiency such as the Mobile Data Terminals found in many civilian police cars. These decrease reaction time and paperwork time for the individual patrolman which decreases the number of responders on shift. While many installations have these systems, most are unable to be used to full effectiveness as locally purchased CAD systems have not evolved with them. The ability to digitally receive, distribute and track responses to incidents and calls for emergency services is a must in emergency management today.

Fourth, these systems lack interoperability with various law enforcement databases and data sources such as state and Federal databases or with Army systems such as the Army Law Enforcement Reporting and Tracking System and installation central alarm and fire detection systems.

Finally, as technology outpaces budget on many installations, maintenance contracts are running out on outdated equipment as there is no lifecycle process in place. Also these current systems are not scalable or upgradable as an installation's situation changes. This threatens to degrade services across our installations. Army-wide CAD will directly interface with information directly from an e911 and Next Gen 911 phone system connection. CAD will auto populate the supplied E911 and Next Gen 911 Automatic Number Identification (ANI) and Automatic Location Identification (ALI) data. This allows instantaneous sharing of information and situational awareness for decision makers.

3.1.4. DOTMLPF-P Constraints, "As-Is" State

Table 2 – DOTMLPF-P Constraints, "As-Is" State

Category	Impact
Doctrine:	• Current CAD systems are not managed by Army NECs on Army networks or adhere to AR 70-1, resulting in numerous IA/Computer Network Defense weaknesses. • Doctrine is developed and maintained individually at the Installation level
Organization:	• Up to 73 installations affected belonging to IMCOM, Medical Command (MEDCOM), Training and Doctrine Command (TRADOC) and Army Medical Command (AMC) • Help desk services are provided by individual local vendors
Training:	• Training is mostly limited to web-enabled resources different for each Installation and locally purchased system. • Annual training requirements are not outlined.
Materiel:	• IT hardware (i.e. computers and printers) are provided as part of each system but are not standardized. Maintenance contracts are running out on many systems and upgrades have not kept up with usage and technology. • Software and software versions are different for each system/installation creating unnecessary costs in maintenance and training.
Leadership and Education:	• Decisions regarding CAD are made locally at the installation Provost Marshal level. While levels of service are outlined by IMCOM, does not standardize systems.
Personnel:	• Qualified personnel are hired through the GS system and are trained on the individual CAD at their installation.
Facilities:	• CAD buildings have additional security concerns and restrictions and CAD systems are separated from other IT systems.
Policy:	• AR 420-1, Army Facilities Management, addresses fire dispatch and response standard, however AR 190-45, Law Enforcement Reporting does not address CAD standards • DoDI 8320.02, Defense Technical Information Center, outlines data sharing over DOD systems. Current CAD systems are not able to adhere to these standards. • IMCOM CLS provide the current standards which installations must meet with their current CAD systems. Non standardized CAD currently meets some of these requirements depending on the installation. • AR 70-1, Army Acquisition Policy, states Army-controlled systems must use a System of Systems approach that leverages aspects of the CIO/G-6 and ASA (ALT) Common Operating Environment (COE) Architecture and the DOD IT Strategy Roadmap.

3.2. "To-Be" Analysis

Employing a common, standardized CAD technical solution will allow for a uniform solution across the Army's installation portfolio improving overall performance while ultimately reducing operational and sustainment costs. A common solution will facilitate the use of common user interfaces and data exchange standards, supporting more effective communications within installations using existing command and control capabilities. A standardized technical CAD solution will also allow for updated, standard doctrine maintained at the Army level, vice varying doctrine developed at the Installation level. This standardized doctrine supports the development of more effective CONOPS, training and sustainment methodologies.

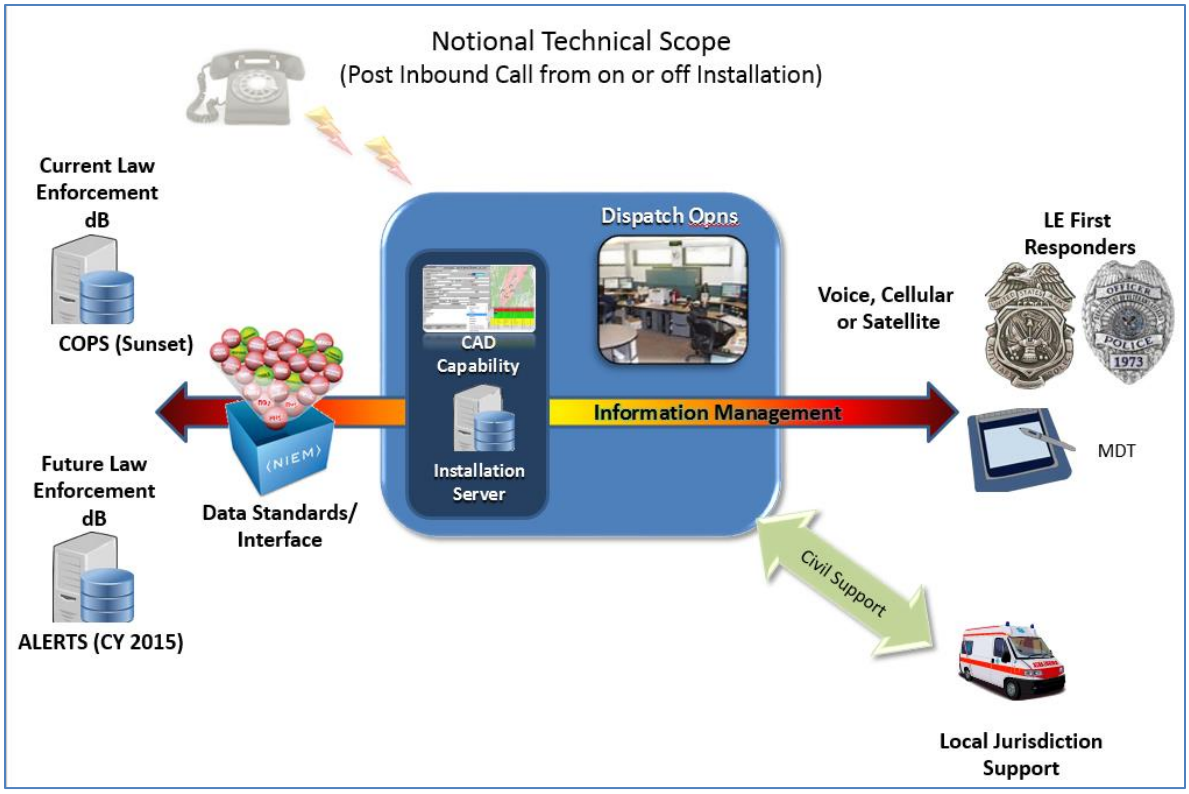
Development and implementation of common training practices ensure improved performance across the inventory and allow for standard position descriptions, personnel hiring and expertise across the Army. In addition, the CAD solution will adhere to the Risk Management Framework (RMF) for DoD Information Technology (IT) DoDI 8510.01, March 12, 2014.

CAD will that interface with land mobile radio, feed a common operating picture to allow resource tracking, and that provides interfaces for information sharing between civilian police, medical and fire agencies adjacent to Army installations.

The Notional Scope depicted in Figure 2, identifies data systems that contain data that needs to be pushed to the first responder as they are being dispatched (weapons registration, prior incidents at that location, etc.) This information needs to be sent to them through an enterprise platform the dispatcher can then push it to that patrolmen to his mobile data terminal.

The information management arrow is a two-way arrow because there is a constant exchange of information during emergency and routine calls from the patrol to the dispatcher. Also there are other systems that contain data that the patrol needs such as access control, National Criminal Information Center (NCIC) data on wants and warrants or local police data. This will be tailored to the installation needs so the system can plug and play into different information management systems tailored to their needs.

Also higher headquarters need visibility of the CAD data to pull statistics such as calls for service or number of patrols dispatched to be able to provide resources appropriately, this data is critical for the law enforcement manpower model.



Notional Technical Scope

Figure 2.

3.2.1. High-Level Outcomes (HLOs)

CAD shall have the capability to collect, modify, store, retrieve, and process record management and geographic information data via a report management function and a record management system. CAD will improve Officer Safety, as the current manual processes will be automated; reducing the chances of critical errors by removing the extensive liability that currently exists with the dispatchers. Additionally, CAD will provide intelligent resources in reporting information that is needed to make knowledgeable business decisions and aid in criminal analysis, helping officer's efforts in providing preventative security measures. Systems must be assessed in relation to responder safety, population safety, the ability to mitigate incident consequences, facilitation of decision making at all levels and be able to be relevant in many situations.

Specifically, the system shall:

• Be fully National Incident Based Reporting System compliant

• Implement a system availability of a minimum of 90 percent when measured on a 24-hour per day, seven day a week basis for 365 days. Processor, disk storage, and power supply redundancy may be required in order to achieve the desired availability and protection of information. The system shall be configured such that operating a training component and/or running reports will not affect system response time.

• Interface with external applications and data sources.

• Have the ability to push the client application via the DHS network to desktops and Mobile Computing Devices via the internal network.

• Allow a user the ability to access the application, download appropriate information and forms relating to incidents, and submit the necessary information without re-keying information.

• Allow the capability to be directly expandable by adding hardware and COTS modules.

• Include a feature for backup, archival and recovery capability without taking CAD out of service and with minimal impact on dispatch operations.

• Provide the capability for users to work offline in the event of connectivity failures, and the capability to continue to work off-line in the event the failure occurs in the middle of a session without any data loss, and to upload saved offline data when connectivity is re-established.

• Contain data exporting capabilities. CAD must have the capability to export data in industry standard database formats to facilitate providing data to other databases controlled by DHS and/or other government entities.

• Be able to generate standard automated forms and templates to be used by all regions; such as incident report, spot report, etc.

• Contain a wide variety of reports and statistical information for analysis and management reporting and/or reporting requirements in real time.

• Allow ad-hoc, dynamically generated reports such that code modifications are not required for each new report.

- Any solutions, materiel or otherwise, must fully comply with DoDI 8100.04, to include requirements described in the DoD Unified Capabilities Requirements (UCR) 2013. Specific requirements related to dispatch are enumerated in 2.12.2.2.3 Enterprise E911 Call Management.
- System must comply with AR 25-400-2, Army Records Information Management System (ARIMS), or its successors.

The focus of this effort is the establishment of a secure computing environment that supports the business processes of US Army Cyber Command. The security provided by the computing environment must be IAW DoD and Department of the Army (DA) Information Assurance policy and guidelines.

DOD SMP Goals/ACP Goal or Objective	HLO Title	HLO Description
SMP Goal 3: Build Agile and Secure Information Capabilities	Interoperability	The CAD will directly interface with information directly from an e911 and Next Gen 911 phone system connection. CAD will auto populate the supplied E911 and NextGen 911 ANI and ALI data. CAD will directly interface with MDT systems, the NCIC, ALERTS and other needed databases. CAD must meet Joint Interoperability Test Command (JITC) certification standards. CAD must also interact and communicate with outside CAD systems in the communities around the installation. A common solution will facilitate the use of common information interfaces and standards, supporting more effective communications using existing command and control capabilities.
ACP 2-1 Deliver Services that Support the Total Force and Protect Installations, People and The Environment		
ACP 4-4 Protect the Army		
ACP 5-2 Equip and Modernize the Army		
ACP 9-0 Sustain and Enhance Business Operations		
SMP Goal 3: Build Agile and Secure Information Capabilities	Communications	CAD will have the maximum number of options in modes of communication with first responders, the public, open source information/social media, outside LE and Emergency organizations and databases.
ACP 2-1 Deliver Services that Support the Total Force and Protect Installations, People and The Environment		
ACP 4-4 Protect the Army		
ACP 5-2 Equip and Modernize the Army		
ACP 9-0 Sustain and Enhance Business Operations		
SMP Goal 3: Build Agile and Secure Information Capabilities	Net-Readiness	

ACP 2-1 Deliver Services that Support the Total Force and Protect Installations, People and The Environment ACP 4-4 Protect the Army ACP 5-2 Equip and Modernize the Army ACP 9-0 Sustain and Enhance Business Operations		The CAD Capability shall satisfy DoD policy concerning system interfaces and policy enforcement controls. This shall include an Enterprise or "Type" accreditation for Army wide use at all installations, Certificate of Networthiness (CONs)//Approved Products List (APLs)/Department of Army (DA) and Local Configuration Control Board (CCBs). The CAD capability will comply with the Joint Information Environment architecture, CIO/G-6 Cloud Computing Strategy and the Army Data Center Consolidation Plan. CAD will be considered for cloud implementation. If local hosting is determined to be appropriate, servers must be located in the approved Installation Processing Node, which may or may not be co-located with the Network Enterprise Center.
SMP Goal 3: Build Agile and Secure Information Capabilities ACP 2-1 Deliver Services that Support the Total Force and Protect Installations, People and The Environment ACP 4-4 Protect the Army ACP 5-2 Equip and Modernize the Army ACP 9-0 Sustain and Enhance Business Operations	GIS	The CAD Capability shall visualize geographic information systems (GIS) data and mapping information while providing accurate real time locations of responder assets.
SMP Goal 3: Build Agile and Secure Information Capabilities ACP 2-1 Deliver Services that Support the Total Force and Protect Installations, People and The Environment ACP 4-4 Protect the Army ACP 5-2 Equip and Modernize the Army	Human Systems Integration	The Provost Marshal Office (PMO) shall include user and administrative level training and a realistic drill scenario standardized across the Army. A first responder who transfers to another installation should be able to step into the new position and function successfully within the CAD dispatch system. CAD must have the capability to provide simulations to support initial and in-service standardized training requirements.

ACP 9-0 Sustain and Enhance Business Operations		
SMP Goal 3: Build Agile and Secure Information Capabilities	Maintainability	The CAD Capability shall allow routine maintenance and patching without significant deterioration of function. The system should be on a regular life cycle of upgrades and replacement.
ACP 2-1 Deliver Services that Support the Total Force and Protect Installations, People and The Environment		
ACP 4-4 Protect the Army		
ACP 5-2 Equip and Modernize the Army		
ACP 9-0 Sustain and Enhance Business Operations		

Table 2a - HLOs

HLO Title	Measurement Criteria				Benefits	Risks	Assumptions (A), Constraints (C), Dependencies (D)
	Measurement	Current (Baseline) Value	Targeted Threshold Value	Targeted Objective Value			
Interoperability	System info sharing across all emergency services and outside agencies. Linkage to all applicable military, local, state and Federal applicable databases	NA	Interoperate with E911 and Land Mobile Radio	Interoperate with Law Enforcement Databases, Local and First Responders	Increased Situational Awareness across all installations and their AO	Shortcomings in information sharing to first responders increasing reaction times. Lack of cooperation with Local jurisdictions may hinder interoperability.	(A) Current CAD systems will not reach networthiness **(C)** Possible incompatibility with existing Law Enforcement and First Responder systems (C) Budget and financial costs **(D)** HQDA and DoD providing IA policy oversight
Communication	Wireless Linkage with MDTs, land mobile radios and modes of information sharing across all emergency services and outside agencies	NA	Hardwire connection to E911, telephone system and LMR servers	Wireless connection to emergency communication systems and local and first responder assets	Increased Situational Awareness of asset distribution across the installation allowing for timely decisions	Shortcomings in information sharing to first responders increasing reaction times and feedback from on scene responders precipitates poor higher level decisions	(A) Some older CAD and communication systems will continue to hinder reaction times **(C)** Possible incompatibility with all systems such as current land mobile net (C) Budget and financial costs **(D)** HQDA and DoD providing IA policy oversight (**D**) Relying on current network infrastructure
Net- Readiness	Accreditation across all installations	NA	100%	100%	Assured network services. Confidentiality, integrity and availability of Army data.	Compromised Army Information Systems. Loss of data through security breach and exfiltration of sensitive data.	**(A)** Computer Aided Dispatch (CAD) capability requires server based approach at each Installation for this ROM **(C)** Budget and financial costs (C) Manpower at NECs **(D)** Interoperability
GIS	Real time GIS Mapping of the incident wirelessly available to responders	NA	100% Real time incident and asset tracking at	100% Real time incident and asset tracking to	Quicker response via instant routing	Lack of real time asset data could lead to inaccurate situational awareness	**(A)** MDTs will have capability to receive this data **(C)** Budget and financial costs **(D)** Accurate Mapping of Installation

			dispatch center	local and first responders assets			
Human Systems Integration	First Responders and dispatchers learn and implement program through in person and simulation training	NA	In person new user training	Training simulation embedded within CAD solution	Provides flexible training options with reference material	Reduced user proficiency and system effectiveness during transition to new system	**(A)** Training and Support Package (TSP) to include drilling will be included with cost of CAD system
							(C) Budget and financial costs (C) Time to conduct training prior to fielding
							(D) System ease of interface (**D**) Availability of new users due to work schedule
Maintainability	System updates and maintenance scheduled periodically	NA	90% system availability	95% system availability	Scheduled maintenance facilitates systems security and enhanced functionality	Degraded effectiveness during down time	**(A)** CAD system will include periodic maintenance
							(C) Budget and financial costs
							(D) Availability of maintenance personnel

Table 2b – HLOs and Measurement Criteria Table

3.2.2. Business Process Re-Engineering (BPR)

The implementation of CAD primarily relates to the Service-to-Satisfaction (S2S) End-to-End (E2E) business process flow. A standardized CAD will enable efficiencies, effectiveness, customer satisfaction, consistency and reductions in operating costs for the delivery of emergency services on garrisons. Additionally, a standardized CAD solution optimizes the quality of service leading to improvements of the Base Operations Support Requirements Model metric inputs and through the utilization of continuous performance improvement (CPI) methodologies. CAD will:

- Facilitate predictable and consistent levels of service to Soldiers, civilians and family members.

- Provide consistency to law enforcement personnel as they are assigned to different installations.

- Enable greater productivity while demonstrating good stewardship of Army and taxpayer resources.

Table 3a – Business Outcomes

HLO Title	Business Outcome	Business Outcome Definition
Interoperability	• Achieve Army Interoperability Certification and Joint Interoperability Test Command (JTIC) certification.	• CAD operates across a multi-agency, multi-jurisdictional environment, as well as "Trust" or Connectivity (CoNs) across Wireless, DoD Wired and Civilian Department of Public Safety (DPS) Networks.
Communication	• Achieve ability to exchange data through various modes of communication (i.e. hardwired and wireless).	Communication linkage with first responders, the public, open source information/social media, outside LE and Emergency organizations and databases.
Net-Readiness	• Achieve RMF Certification	• RMF Certification achieves all Net-Readiness requirements
GIS	• Geofile Synchronization • Location Validation • Asset Routing • Manual Location Entry • Topologically Integrated Geographic Encoding and Referencing (TIGER) files	• CAD Capability shall support the creation and maintenance of a synchronized Geofile using an available mapping/GIS database • CAD Capability shall verify incident location against the Geofile to determine its exact location • CAD Capability shall generate a route between asset locations and incident location • CAD Capability shall support the ability to manually enter event location details. • Ability to map emergency response districts for police, fire and Emergency Management Service (EMS) using US census TIGER (like) shape and line data
Human Systems Integration	• Training	• The PMO shall include User and Administrative level training and a realistic drill scenario.
Maintainability	• Maintain Data Availability	• The CAD Capability shall allow routine maintenance and patching without significant deterioration of function.

Table 3b – Business Outcomes and E2E Alignment ("To-Be" State)

Business Outcome	E2E/BEA Perspective		
	Business Flow	Business Process	Business Capability
Achieve Army Interoperability Certification and Joint Interoperability Test Command (JTIC) certification.	Acquire-to-Retire	Concept-to-Product	Accredited Emergency Service across the force
Achieve ability to exchange data through various modes of communication (i.e. hardwired and wireless).	Acquire-to-Retire	Concept-to-Product Cost Management	Effective Communications
Achieve RMF Certification	Acquire-to-Retire	Concept-to-Product	Policies Match Usage
• Geofile Synchronization • Location Validation • Asset Routing • Manual Location Entry • Topologically Integrated Geographic Encoding and Referencing (TIGER) files	Acquire-to-Retire	Concept-to-Product	• Real time location services • Mapping
Training	Acquire-to-Retire Market-to-Prospect	Hire to Retire Cost-Management	Program of Instruction (POI) in place
Maintain Data Availability	Acquire-to-Retiree	Cost-Management	Secure in the Army Enterprise

Table 3c – Business Outcomes and Measurement Criteria ("To-Be" State)

Business Outcome	Measurement Criteria				Benefits	Risks	Assumptions (A), Constraints (C), Dependencies (D)
	Measurement	Current (Baseline) Value	Targeted Threshold Value	Targeted Objective Value			

• Achieve Army Interoperability Certification and Joint Interoperability Test Command (JTIC) certification.	• Standardized Army-Wide CAD Interoperability Certification	N/A	• 100%	• 100%	• Integrity and security of data at rest • Reduction in certification costs	• Disclosure of LE classified information and PII • USACC goals are not met	**(A)** Single, standardized CAD solution **(C)** Public Key Infrastructure (PKI) authentication enforced by system owners **(D)** PKI digital certificates
• Achieve ability to exchange data through various modes of communication (i.e. hardwired and wireless).	• % of Infrastructure Communications (Hardwire connection to E911, telephone system and LMR servers) • % of Mobile Asset Communication (i.e. wireless connection to emergency communication systems and local and first responder assets)	• N/A	• 100% • 80%	• 100% • 90%	• Trusted business operations • Data exchange with multiple assets and systems	• Compromised Army Information Systems	(A) Limits on communication with rapidly changing technology (C)Funding
• Achieve RMF Certification	• Standardized Army-Wide RMF certification	• N/A •	• 1000% •	• 1000% •	• Single certification process to operate on all Installations • Standard Implementation • Reduction in certification costs	• Unknown RMF process flow and durations	**(C)** (A) Single, standardized CAD solution

• Geofile Synchronization • Location Validation • Asset Routing • Manual Location Entry • Topologically Integrated Geographic Encoding and Referencing (TIGER) files	• % Delivery of real time incident and asset tracking at dispatch center • % Delivery of real time incident and asset tracking to local and first responders assets	N/A N/A	• 100% 80%	• 100% 90%	• Faster response time • Increased situational awareness	• Installation infrastructure (i.e. bandwidth limitations)	**(A)** Mapping data exists for Installation and local Jurisdictions in a compatible format
• Training	• % of people receiving new user training	• N/A	• 80%	• 100%	• Standardized training across all Installations	• Installation staff availability and turnover	(A) Training provided by contracted vendor will be on a rotational basis during fielding with enough time to complete prior to implementation (C) One training event (multiple sessions) per Installation **(D**) Installation staff availability

• Maintain Data Availability	• % of time system data is available	• N/A	• 90% availability	• 95% availability	• Secure environment • Up to date software • Additional functionality/capability	• • Improperly applied patch can disable functionality • Downtime can hinder response times	(A) Updates and patches installed by Installation NEC. (D) Availability of NEC personnel to apply updates and patches

3.2.3. DOTMLPF-P Impact, "To-Be" State

Table 4 – DOTMLPF-P Impacts, "To-Be" State

Category	Impact
Doctrine:	• CAD systems are managed by Army NECs on Army networks and adhere to AR 70-1, resulting in being a part of the IA infrastructure with lifecycle replacement and upgrades. • Single ATO/CON accreditation • Develop and implement common employment and sustainment doctrine for single technology, which will drive common, standardized CONOPS
Organization:	• The 73+ installations affected belonging to IMCOM, MEDCOM, TRADOC and AMC are on a standardized CAD system that is managed cradle to grave • Single help desk service provided by the Army IT framework.
Training:	• Training is standardized and codified across all installations and can have employees trained within 2 weeks. • Annual training requirements are outlined and simulation capable CAD will assist with in-service training of operators and responders on a set schedule. • Development and implementation of uniform training practices ensure improved performance across the inventory
Materiel:	• Common, standardized technical solution employed across Army Installations interoperable with response paradigm • IT hardware (i.e. computers and printers) and software are provided as part of each system and are standardized. Maintenance contracts are managed on the Army lifecycle management model and systems are kept upgraded as new and evolving technologies improve efficiencies in CAD.
Leadership and Education:	• Decisions regarding CAD are made by Army Commands, Army Supporting Commands and Direct Reporting Units and are standardized
Personnel:	• Position Descriptions are standardized across Army to allow uniform hiring across the Army • Qualified personnel are hired through the GS system, or provided by contract support, are trained to operate the standardized CAD solution deployed to all installations. . Currently existing personnel will train and run the new CAD
Facilities:	• CAD buildings have additional security concerns and restrictions and CAD systems are separated physically but linked to the Army Enterprise. Existing structures can be used.

Policy:	• AR 190-45, Law Enforcement Reporting is updated to address new CAD standards • CAD will comply with DoDI 8320.02, Defense Technical Information Center andoutlining data sharing over DOD systems. • CAD will comply with IMCOM CLS provide the current standards which installations must meet with their current CAD systems. • CAD will comply with AR 70-1 using a System of Systems approach leveraging the CIO/G-6 and ASA (ALT) COE Architecture and DOD IT Strategy Roadmap • CAD will comply with AR 525-2 The Army Protection Program

3.3. Recommended Course of Action

Obtain Investment Review Board (IRB) approval of the Problem Statement and continue the analysis to identify a material solution that supports the Army PMO/DES need for a secure and trusted data processing environment to dispatch first responders, interact with adjacent emergency services and link in with e-911.

3.4. Rough-Order-of-Magnitude (ROM) Cost Estimate

Results are presented from the ROM cost estimate of the funding requirements to implement a material solution that will provide a secure computing and processing environment through existing solutions. The ROM cost analysis assumes a 15-year lifecycle, one tech refresh cycle, and a sustainment period of 10 years post Full Operational Capability (FOC) to a total Army 70 installations. The estimate includes costs for procurement, testing, fielding, personnel training, technical refresh, sustainment licensing and technical support. Costs are comprehensive to a program to provide the material solution for meeting and sustaining requirements for new hardware in the data center and in the field. It was assumed the program will be executed through a Program Office and require an initial year of RDTE effort, seven years of Program Office support, and 10 years of sustainment after achieving FOC. Two years of initial sustainment costs are included in the procurement costs. An additional detailed listing of three appropriations, RDTE, OPA, and OMA are provided in table format. The ROM estimate was produced using ACEIT 7.4 and is presented with confidence limits (CL) after applying price risk methods. The High 75 percent CL, Medium 50 percent CL, and Low 40 percent CL estimates were calculated using Monte Carlo simulations with POST 7.4 for each appropriation. Values are presented in Then-Year (TY) $M at the 50 percent CL.

ROM (HIGH): $539.5M 15-Year Lifecycle = $233.6M Implementation (Y1-Y3), $305.9M sustainment (Y4-Y15)

ROM (MED): $487.2M 15-Year Lifecycle = $208.6M Implementation (Y1-Y3), $278.6M sustainment (Y4-Y15)

ROM (LOW): $465.2M 15-Year Lifecycle = $197.1M Implementation (Y1-Y3), $268.1M sustainment (Y4-Y15)

Appropriation details are presented below.

Cost Estimate TY$M

CAD ROM Estimate

Confidence Interval

	40% CL	50% CL	75% CL
Total	465.2	487.2	539.5
RDTE	6.4	6.7	7.4
OPA	190.7	201.8	226.1
OMA	268.1	278.6	305.9

Appendix D.
Charleston County and JB CHS MOU

MEMORANDUM OF AGREEMENT
Between
CHARLESTON COUNTY, SOUTH CAROLINA
and
JOINT BASE CHARLESTON
for
SHARED SERVICES INCLUDING TRANSITION OF AN ENHANCED 9-1-1
PRIMARY PUBLIC SAFETY ANSWERING POINT
AGREEMENT NUMBER (FB4418-17048-201)

This is a Memorandum of Agreement (MOA) entered into this 17th day of February, 2017, between Charleston County, South Carolina (hereinafter referred to as "the County"), and Joint Base Charleston (hereinafter referred to as "JB CHS"), its successors and assigns, collectively referred to as the "Parties." The division of the County involved in this agreement is Charleston County Consolidated Dispatch Center (hereinafter referred to as "CDC").

WHEREAS, the Parties desire to enter into this MOA to transition the JB CHS enhanced 9-1-1 Primary Public Safety Answering Point ("PSAP") call taker responsibilities and routing of the emergency information to the CDC to benefit the civilian and military personnel working and/or residing on JB CHS;

WHEREAS, the shared services set forth in this MOA allow for enhanced information sharing and situational awareness generally benefitting public safety agencies serving the Charleston and Berkeley County communities; and

WHEREAS, the intergovernmental agreement for consolidating 9-1-1 services established the Charleston County Consolidated Dispatch Board (the "Board"), which includes multi-jurisdictional representation from law enforcement, fire and emergency medical services entities within Charleston County; and

WHEREAS, the Board has guided the process of consolidated 9-1-1 emergency response communications, increased interoperability and information sharing among agencies through technological advances and further recommends the expansion of CDC shared systems/services with JB CHS;

NOW, THEREFORE, in consideration of the mutual terms, conditions, promises, and covenants set forth, the Parties hereto agree as follows:

ARTICLE 1. PURPOSE AND INTENT:

1.1. It is the purpose and intent of this MOA to transfer public safety answering point (PSAP) functions and responsibilities (as outlined in Section 3.1) of JB CHS to the CDC PSAP. CDC PSAP would then be designated and authorized to receive emergency 9-1-1 calls

requesting public safety services (i.e., law, fire, medical, etc.), including areas of JB CHS located within both Charleston and Berkeley Counties.

1.2. It is the purpose and intent of this MOA to maintain all dispatching functions of JB CHS Fire Emergency Services and Security Forces in their present state on JB CHS through the Emergency Communication Center ("ECC") unless otherwise noted in this document.

1.3. It is the purpose and intent of this MOA that the County will take all JB CHS emergency 9-1-1 calls, and that each party shall only be liable for payment of that portion of any liability, costs, expenses, demands, settlements, or judgments resulting from the negligence of its own agents, officers and employees.

1.4. It is the purpose and intent of this MOA that both parties will mutually benefit from the sharing of services.

1.4.1. Currently JB CHS receives wireline 9-1-1 calls only. Others go to CDC and Berkeley County 9-1-1. Under this MOA, 9-1-1 calls at JB CHS (Wireline, Wireless, Text and other means as they become available) will go to one central answering point.

1.4.2. JB CHS services continue to be dispatched by JB CHS personnel with local standard operating procedures and base geographic knowledge.

1.4.3. Information Sharing and enhanced situational awareness will benefit JB CHS public safety responders and other local public safety agencies and will assist in reducing response time.

1.4.4. Charleston County can, as set forth in Section 3.2.3, provide backup facilities for JB CHS dispatch in the event JB CHS must relocate to a backup center.

1.4.5. The Parties will also benefit from improved interoperability, training and cross-information flow.

ARTICLE 2. AUTHORITY: This MOA is governed by DoDI 6055.17, *DoD Installation Emergency Management (IEM) Program*, January 13, 2009 and AFMAN 33-145, *Collaboration Services and Voice Systems Management*, 6 September 2012.

ARTICLE 3. RESPONSIBILITIES OF THE PARTIES:

3.1. County will -

3.1.1. Answer all 9-1-1 calls (i.e., wireline, wireless & text, etc.) placed from within the jurisdiction of JB CHS.

A. This includes areas of JB CHS located within both Charleston and Berkeley Counties.

B. The CDC will not routinely transfer calls to JB CHS. However, should an unusual circumstance occur where JB CHS wants or needs to speak to a specific caller, the call will be transferred to JB CHS when requested by the JB CHS ECC.

3.1.2. Question the caller in accordance with CDC Standard Operating Procedures ("SOPs") and Protocols.

3.1.3. Enter information obtained from the caller into the computer aided dispatch (CAD) system.

3.1.4. Electronically transfer CAD data to JB CHS ECC.

A. The initial incident will be sent to the JB CHS Dispatcher's CAD Call Pending Queue.

B. Additional/updated information will be entered into the CAD incident comments.

3.1.5. Communicate with Berkeley County Dispatch when a medical incident occurs in Berkeley County's jurisdiction of JB CHS.

3.1.6. Dispatch Charleston County EMS when a medical incident occurs or as requested by JB CHS in Charleston County's jurisdiction of JB CHS.

3.1.7. Allow the JB CHS ECC unit to relocate to one of the CDC locations (primary or backup) and utilize consoles if CAD system is inoperable or other circumstances occur that would warrant relocation of dispatch as mutually agreed upon by the Parties.

3.1.8. Operate under the authority of the Charleston County Consolidated Dispatch Board who determines the Center's operational procedures and the parameters of public safety information sharing available through the CDC.

3.1.9. Record and retain call audio and incident data information in accordance with CDC procedures.

3.1.10. Subject to all Federal, State, and local laws, consider all recordings, data and information obtained regarding JB CHS incidents as property of the JB CHS and will not be released without prior written approval of JB CHS authorized person(s) (as indicated in paragraph 3.2.7) who shall document coordination of JB CHS Legal and Public Affairs Offices (628 AWB/PA and 628 ABW/JA).

3.1.11. Maintain the Charleston County Interagency Network, CAD and Alastar Suite of Shared Technology Systems available at the JB CHS, subject to the costs outlined in Attachment A.

3.2. JB CHS will -

3.2.1. Maintain JB CHS ECC operations (physically on the base) and receive the electronic transfer of CAD data from the CDC.

3.2.2. Dispatch the appropriate Fire Emergency Services and/or Security Forces response in accordance with JB CHS operational procedures. When assistance from Law or Fire emergency response agencies outside of Charleston County is desired, JB CHS will communicate directly with these agencies (or their communications centers).

3.2.3. The JB CHS agrees to continue to maintain its own ECC for the dispatching of its emergency response units to incidents in or near the JB CHS, and acknowledges that the CDC will not have responsibility for dispatching its units on a day-to-day basis. Only in extreme emergency situations (i.e., extreme weather) will the JB CHS request the CDC to dispatch its units, to include situations in which the JB CHS ECC staff is unavailable. It is understood that the CDC will agree to this request as long as the CDC has the capacity to do so in such extreme situations as determined by the CDC.

3.2.4. Provide initial and updated geographic information to the CDC.

3.2.5. Work with the CDC to resolve geographic information discrepancies.

3.2.6. Recognize that the Charleston County Consolidated Dispatch Board has operational authority for the CDC, and in that capacity the Board determines the CDC's operational procedures and the parameters of public safety information sharing available through the CDC.

3.2.7. Provide and update the CDC with the name(s) of the person(s) authorized to receive and release recordings, data and information regarding incidents that occur on the JB CHS.

3.2.8. As the owners of historical recordings, data and information, respond to Federal and State Freedom of Information Act (FOIA) requests as required by law.

3.3. Both parties will -

3.3.1. Transmit all communication between CDC's Call Takers and JB CHS's dispatchers through:

A. Primary-CAD.
B. Secondary-Telephone.
C. Tertiary-Radio (through the Charleston County 800mhz Radio System, already in use by the JB CHS).

ARTICLE 4. SCOPE OF SERVICES:

4.1. It is understood that ongoing cooperation/coordination of JB CHS staff is essential, to accomplish items included in the Scope of Work (SOW) outlined in Attachment B, the responsibilities in the attached SOW fall primarily on CDC staff.

4.1.1. Both agencies will appoint a Project Manager to implement this MOA, and each Party will notify the other of any changes in the Project Manager.

4.1.2. Both Parties will appoint a primary and secondary technical point of contact, and each Party will notify the other of any changes in the primary and secondary technical points of contact.

4.1.3. All items in Attachment B must be complete prior to transition of PSAP call taking to the CDC.

4.2. The following technology will be shared with JB CHS, subject to the costs outlined in Attachment A -

4.2.1. Charleston County Interagency Network with secured and encrypted AT&T ASE Circuits.

4.2.2. Charleston County CAD - Connection will be through the above mentioned Charleston County Interagency Network.

4.2.3. Alastar (GIS based information sharing and situation awareness tool).

4.2.4. Next Generation 9-1-1 (NG9-1-1) Internet Protocol (IP)-based system(s) as it becomes available.

4.3. The implementation of Shared Systems will involve installation of equipment as listed in Attachment B.

4.3.1. JB CHS agrees to provide 4 U rack space and power for the above equipment listed in Attachment B.

4.3.2. JB CHS agrees to provide network connectivity between JB CHS facilities to support this effort.

4.3.3 The Parties agree that the County maintains ownership of the Interagency Network associated hardware equipment described in Attachment B, and this equipment will be returned to the County upon the expiration or termination of this Agreement, whichever occurs earlier.

4.3.4 JB CHS agrees to provide County representatives with 24-hour access to the inter-agency network node equipment listed above (for trouble-shooting and repair).

4.3.5 The County agrees to provide 24-hour trouble-shooting for CAD related issues.

4.3.6 JB CHS agrees to maintain access to the Charleston County Radio System.

ARTICLE 5. TERM AND TERMINATION:

5.1. Unless further amended or earlier terminated in accordance with this MOA, the term of this MOA will continue through September 30, 2019, with installation work commencing on or about September 1, 2016 and the transition of all 9-1-1 calls on or about February 1, 2017.

5.2. Either Party, by advance written notice, may terminate this Agreement in whole or in part in the event sufficient appropriations of funds from any source (whether federal, state, County or other source) are not made available or sufficient funds are otherwise unavailable, in either case, to pay the costs under this agreement. Otherwise, termination of this Agreement will take place only under extraordinary circumstances as mutually determined by both Parties, to include but not limited to failure or refusal of either Party to perform the duties and obligations outlined in this Agreement. If practicable, the terminating Party shall provide 90 days written notice to the non-terminating Party.

ARTICLE 6. FINANCIAL COMMITMENTS:

6.1. The Parties agree to move forward with all funding criteria as set forth in Attachment A (Start-up costs and Annual Costs) to complete all items listed in ARTICLE 4, Scope of Services and Attachment B, Scope of Work for Consolidated Dispatch Shared Services with JB CHS:

6.2. The Parties agree that the funding chart shown in Attachment A provides the amount that JB CHS shall pay for start-up costs and for the annual year starting on 1 October 2017 (Federal Fiscal Year 17). It is understood that for Federal Fiscal Years 2018 and 2019, this chart shows the anticipated increases estimated at 3% per year. Should the actual increase in cost from one fiscal year to the next exceed an overall 5% increase (also shown),

Charleston County may request an amendment to this agreement in order to recoup the additional increased cost.

6.3. For those expenses reimbursable (percentage based) by 9-1-1 funding, Charleston County will pass along only those costs not reimbursed through 9-1-1 funds.

6.4. Payment to Charleston County for this agreement will be processed through via Direct Deposit/Electronic Funds Transfer (DD/EFT).

ARTICLE 7. CHANGES IN SCOPE OF SERVICES: Any change to the Scope of Services must be accomplished by a written amendment, executed by the parties in accordance with ARTICLE 9.1.

ARTICLE 8. GOVERNMENTAL IMMUNITY: The Parties are entitled to the privileges and protections of sovereign immunity, and agree to be fully responsible for the negligent acts and omissions of their agents or employees to the extent permitted by law. Nothing herein in this Article is intended to serve as a waiver of sovereign immunity by any party to which sovereign immunity may be applicable. Nothing herein shall be construed as consent to be sued by third parties in any matter arising out of this Agreement or any other contract.

ARTICLE 9. MISCELLANEOUS:

9.1. No modification, amendment, or alteration in the terms or conditions contained in this Agreement shall be effective unless contained in a written document prepared with the same or similar formality as this Agreement and executed by the County and JB CHS.

9.2. Neither the County nor JB CHS intend to directly or substantially benefit a third party by this Agreement. Therefore, the Parties agree that there are no third party beneficiaries to this Agreement and that no third party shall be entitled to assert a claim against either of them based upon this Agreement. The Parties expressly acknowledge that it is not their intent to create any rights or obligations in any third person or entity under this Agreement.

9.3. Whenever either party desires to give notice to the other, such notice must be in writing, sent by certified United States Mail, postage prepaid, return receipt requested, or by hand-delivery with a request for a written receipt of acknowledgment of delivery, addressed to the designated point of contact. The position/address for giving notice shall remain the same as set forth herein until changed in writing in the manner provided for in this section. For the present, the parties designate the following:

FOR THE COUNTY:

Keith Bustraan, Charleston County Administrator
4045 Bridge View Drive
North Charleston, SC 29405

With Copies to:

Jim Lake, Director, Charleston County Consolidated 9-1-1 Center
8500 Palmetto Commerce Parkway, N. Charleston, SC 29456
FOR JB CHS:

FOR JB CHS:

Robert K Lyman, 628th Air Base Wing Commander
Joint Base Charleston, South Carolina 29404

With Copies to:

Matthew S. Brennan, Lt Colonel, 628th Civil Engineer Squadron
Joint Base Charleston, South Carolina 29404

Joshua M. Aultman, Major, 628th Communications Squadron
Joint Base Charleston, South Carolina 29404

Robert N. Clouse, Lt. Colonel, 628th Security Forces Squadron
Joint Base Charleston, South Carolina 29404

Judy P. Driggers, 628th Air Base Wing Support Agreement Manager
Joint Base Charleston, South Carolina 29404

9.4. Neither this Agreement nor any interest shall be assigned, transferred, or encumbered by either party.

9.5. Resolution of Disputes: All disputes arising out of or related to this Agreement will be resolved in accordance with paragraphs 1.1-1.4 of this agreement. The parties to this Agreement should attempt to resolve disputes between themselves at the lowest level. First, the dispute should be addressed by the 628th Civil Engineer Squadron Commander (CES/CC) and Director of Charleston County Consolidated 911 Center). If the dispute still cannot be resolved, then the dispute will be forwarded to the signatories of this agreement, 628th Air Base Wing Commander (ABW/CC) and the County Administrator. If the signatories to this agreement cannot resolve the dispute, either party can submit a written appeal addressed to the Deputy Assistant Secretary of the Air Force (Installations).

9.6. Decision by the Reviewing Official: The Deputy Assistant Secretary of the Air Force (Installations) must, within thirty (30) days of the receipt of the dispute, notify the parties of the decision. This decision shall be binding on the parties

9.7. Agency Decision: The decision on the appeal of the Deputy Assistant Secretary of the Air Force (Installations) or his/her duly authorized representative is final and conclusive. Nothing in this Agreement may be interpreted to deny or limit the local government the right thereafter to seek relief in the applicable federal court.

9.8. Continuation of Work: Pending the resolution of any such dispute, work under this Agreement not subject to dispute may continue as specified by agreement between the parties.

9.9. Subject to paragraphs 9.5-9.7, litigation disputes arising out of or related to this Agreement will be resolved in the federal district of South Carolina. The laws of South Carolina shall govern this contract.

9.10. Should any part of this MOA be determined by a Court of competent jurisdiction to be invalid, illegal, or against public policy, said offending Section shall be void and of no effect and shall not render any other Section herein, nor this MOA as a whole, invalid. Any terms which, by their nature, should survive the suspension, termination or expiration hereof shall be deemed to survive.

IN WITNESS WHEREOF, the Parties have made and executed this Agreement on the respective dates under each signature: Keith Bustraan, County Administrator for Charleston County (THE COUNTY) and Robert K Lyman, 628th Air Base Wing Commander Joint Base Charleston, South Carolina 29404 (JB CHS).

FOR CHARLESTON COUNTY:

WITNESSES

James E. Mitchell Buell

02-17-17

C Bustraan (Seal)
Keith Bustraan, County Administrator

DATE: 2/17/17

FOR JOINT BASE CHARLESTON:

WITNESSES

Vivica N. Bryant

02-16-17

Robert Lyman (Seal)
Robert K. Lyman, 628th Air Base Wing Commander

DATE: 16 Feb 2017

Attachment A - Costs

ATTACHMENT A - Text updated 11/21/16 - Costs updated 8/1/2016

JB CHS Shared Services Startup Cost	
	Fed FY- 16
Start-up Costs	JB CHS Pays CDC
CAD Licenses (x2)	$4,000
ASE/SCRA Costs (equip & conf)	$920.00
Priority Dispatch EMD Cardset	$86.80
Priority Dispatch EFD Cardset	$434.00
Priority Dispatch EPD Cardset	$544.00
ASE Network turn-on/testing	$1,000.00
Tel Priority Service Start-up	$28.00
Additional Network/Admin	$1,565.00
Total Start-up Cost	**$8,578**

JB CHS Shared Services Annual Cost					
	Fed FY 17	Fed FY 18		Fed FY 19	
Annual Costs	**Actual**	**@ 3%**	**@ 5%**	**@ 3%**	**@ 5%**
Operational Costs	$6,677	$6,877.31	$7,010.85	$7,083.63	$7,221.18
Staff /Admin Costs	$11,439	$11,782.17	$12,010.95	$12,135.64	$12,371.28
Additional Network/Admin	$15,192	$15,647.76	$15,951.60	$16,117.19	$16,430.15
Annual Cost	**$33,308**	**$34,307.24**	**$34,973.40**	**$35,336.46**	**$36,022.60**

Notes:

1) ASE/SCRA Costs: Equipment to be purchased/installed/configured at JB CHS includes Router, Switch and Encryption Device.
2) Additional Network/Admin: Includes JB CHS requested Firewall, 2nd switch for JB CHS dispatch backup site and Internet (for Alastar Access), manufacturer's maintenance and SCRA monitoring/maintenance, plus CDC Indirect costs.
3) JB CHS is providing their own connectivity between their primary and backup dispatch sites.

Note: For a more detailed Annual Cost spreadsheet, contact CDC Account Technician at 843-529-3700

Attachment B

Scope of Work for Consolidated 9-1-1 Center Shared Services with JB CHS:

While it is understood that ongoing cooperation/coordination of JB CHS staff is essential, unless otherwise indicated in the SOW outlined below, the responsibilities in this SOW fall primarily on CDC staff. The Technical Project Manager/Technical point of contact for the CDC will be Michael Ball, 9-1-1 Technology Manager, with Matt Hibler as secondary in these roles. The Technical contact for the JB CHS will be Master Sergeant John Miele, Assistant Chief of Operations, with 628 Civil Engineer Squadron and Technical Sergeant Lee Fast, NCOIC, Emergency Communication Center as the secondary technical contact.

I. Network
   a. Charleston County Interagency Network (through AT&T ASE):
      i. CDC: Place Order with AT&T for 10 MB ASE connection with request for AT&T installation on or about September 1, 2016 (order placed on 6/28/16).
      ii. CDC: Purchase and configure equipment for ASE connection and commercial internet service.
      iii. Joint responsibility: The following equipment will be installed at the JB CHS at agreed upon locations:

Make	Qty	Description
CERTES Networks	1	Ethernet multi-layer network encryption and authentication appliance - 1U form factor 10 Mbps bandwidth available.
Cisco	1	Router
Dell	2	Switch, Dell PowerConnect
Cisco	1	Firewall
Internet	1	Provide a 10 Mbps (minimum) commercial internet service

NOTE: CERTES TrustNet software and bandwidth license for one CEP10-VSE appliance will be included.

      iv. Joint responsibility: Configure and test on existing Network during prior to go-live date.
      v. Go-Live goal date is on or about February 1, 2017 (dependent upon installation date of ASE).
      vi. CDC: Configure, test and maintain firewall for JB Interagency Network node.

II. Telephony/Text
   a. 9-1-1 Wireline
      i. Joint responsibility: Move all JB CHS Wireline 9-1-1 to Charleston County
      ii. CDC: Notify & coordinate with AT&T for move on specific date
      iii. Joint responsibility: Transfer Line
         1. ID line to transfer 9-1-1
         2. Implement and test
   b. 9-1-1 Wireless
      i. Joint responsibility: Move all JB CHS Wireless 9-1-1 to Charleston County
         1. Verizon

2. AT&T
3. T-Mobile
4. Sprint

c. Text to 9-1-1
   i. Joint responsibility: Move all JB CHS Text to 9-1-1 to Charleston County
      1. Verizon
      2. AT&T
      3. T-Mobile
      4. Sprint

d. Ten-Digit Telephony - Joint responsibility
   i. Identify Public Non-Emergency Number
   ii. Identify PSAP to PSAP only Number for all sites involved

III. Radio - CDC:

a. Identify JB CHS Charleston County Talkgroups/Channels
   i. Fire
   ii. Law

b. Program and test in CDC Consoles

c. Identify Talkgroup/Channels JB CHS to use when contacting CDC

IV. Computer Aided Dispatch (CAD)

a. Licenses
   i. CDC will purchase 2 CAD licenses on behalf of JB CHS, and then charge JB CHS their 9-1-1 non-reimbursable share.
   ii. CDC, in cooperation with JB CHS, will Install/test

b. Hardware
   i. JB CHS to purchase/acquire/install Inform CAD Workstation with the following Specifications:
      1. Computer configuration: Business Workstation class machine
      2. Processor: one dual core 2.0 GHz or faster processor minimum
      3. RAM: 4 GB recommended
      4. Disk: 120 GB minimum
      5. Operating System: Windows 7 32 bit or 64 bit
   ii. Setup/testing of Hardware with CAD system *(Both Center and JB CHS involved)*

c. Data Files for CAD Entry
   i. JB CHS to provide the following data about their operation)
      1. Law
         a. Personnel
         b. Vehicles
      2. Fire
         a. Personnel
         b. Vehicles
         c. Hydrants
         d. Response Plans

V. Geographic Information (GIS)

a. JB CHS GIS Data - CDC
    i. Obtain and review for completeness
    ii. Work with Berkeley County for GIS Data applicable to JB CHS portions in Berkeley County
    iii. Resolve Data discrepancies
    iv. Install & test
b. Premise and Common Name Data
    i. Obtain
    ii. Install & test

VI. Alastar Situational Awareness tools
a. Provide access for 3 user accounts

VII. SOPs
a. CDC will Develop SOPs for the following:
    i. Call Answering
    ii. Incident Transfer via CAD
    iii. Radio Dispatch
    iv. Backup - Failure of Technology

VIII. Training
a. **CDC Staff Training**
    i. Call Taker Orientation to JB CHS Geography
    ii. Provided by CDC and JB CHS staff
b. **Berkeley County 9-1-1 Center Training**
    i. CDC staff to ensure Berkeley County staff are fully aware and trained on changes impacting them
    ii. Provided by CDC staff
c. **JB CHS Staff Training**
    i. Emergency Telecommunications Course - Optional
        1. Standard/Best Practice
        2. 40 hours of training per person
        3. In person course at the CDC
        4. Provided by CDC staff
    ii. CAD training
        1. Required to operate CAD
        2. Up to 16 hours of training per person
        3. In person course at the CDC and/or JB CHS
            a. Location based on timing of the installation and convenience of the participants
        4. Provided by CDC staff and train-the-trainer
    iii. Security Awareness Training
        1. South Carolina Law Enforcement Division (SLED) and Criminal Justice Information System (CJIS) requirement
        2. Approximately 2 hours of training per person
        3. On-line course

iv. South Carolina Criminal Justice Training Academy (SCCJTA)Training - Optional
    1. South Carolina State Law requirement
    2. 80 hours of training per person
    3. In person course at the SCCJTA
    4. Will be sought, although it is recognized that scheduling will be challenging and therefore may be delayed.
v. Alastar
    1. Required to operate Alastar
    2. 4 hours of training per person
    3. In person course at the CDC and/or JB CHS
        a. Location based on timing of the installation and convenience of the participants
    4. Provided by CDC staff and train-the-trainer
vi. 9-1-1 Center Observation
    1. Optional upon request
    2. Flexible hours with agreed upon schedule
    3. CDC will encourage and allow observation (aka shadowing) of CDC Telecommunicators by JB CHS dispatchers to better understand the call flow

IX. Public Education
a. Shared/cooperative responsibility of JB CHS and CDC to educate on:
    i. Who & When to Call
    ii. Call Process
    iii. Text to 9-1-1
    iv. Smart911

X. Go-Live

DEPARTMENT OF THE AIR FORCE
HEADQUARTERS 628TH AIR BASE WING (AMC)
JOINT BASE CHARLESTON SC

31 January 2017

MEMORANDUM FOR 628 ABW/CC

FROM: 628 ABW/JA

SUBJECT: Legal Review of Memorandum of Agreement between the 628th Air Base Wing, Joint Base Charleston, South Carolina and Charleston County, South Carolina

1. **BLUF:** We find the submitted the Memorandum of Agreement (MOA) for legal sufficient.

2. **FACTS:** The purpose of the agreement is to transfer the Joint Base Charleston (JB CHS) 911 Primary Public Safety Answering Point (PSAP) call taker responsibilities and routing of the emergency information to the Charleston County Consolidated Dispatch Center (CDC). The intergovernmental agreement establishes the Charleston County Consolidated Dispatch Board (Board), which includes multi-jurisdictional representation from law enforcement, fire and emergency medical services. The transfer will allow for the enhanced information sharing and situational awareness generally benefitting public safety agencies serving the Charleston and Berkeley County communities and the JB CHS community.

3. **LAW AND ANALYSIS:**

a. Department of Defense Instruction (DoDI) 4000.19, *Support Agreements*, dated 25 April 2013, and Air Force Instruction (AFI) 25-201, *Intra-Service, Intra-Agency, and InterAgency Support Agreements Procedures*, dated 18 October 2013, govern this agreement. The instruction allows for memorandums of understanding or agreement when beneficial to parties. DoDI 4000.19 provides that support agreements document the terms of an agreement that a DoD component enters into with a State or local government (DoDI 4000.19, Enclosure 3, paragraph 1(a)). Memorandums of various types are used to document the requirements of the agreement between the parties. Furthermore, DODI 6055.17, *DOD Installation Emergency Management (IEM) Program,* and AFMAN 33-145, *Collaboration Services and Voice Systems Management*, also apply to this particular MOA.

b. I note that this MOA has gone through numerous iterations with JA comments and edits. Ms. Erin Dixon and Capt Willis Brown were working closely with the interested parties as well as SAF/GC. After reviewing the previous comments and the revised MOA, there was only one minor comment: The dates in the first paragraph need to be revised to reflect the current month and year.

4. **RECOMMENDATION:** I find that the proposed MOA adequately explains the agreement between the parties and is legally sufficient. If you should have any questions or concerns, please contact the legal office at (843) 963-5502.

REB

ROBERT E. BEYLER, Civ, DAF
Chief, Administrative Law Division

DEPARTMENT OF THE AIR FORCE
WASHINGTON, DC

OFFICE OF THE SECRETARY

AFMAN17-1202_AFGM2016-01

4 November 2016

MEMORANDUM FOR DISTRIBUTION C
MAJCOMs/FOAs/DRUs

FROM: SAF/CIO A6
1800 Air Force Pentagon
Washington DC 20330-1800

SUBJECT: Air Force Guidance Memorandum (AFGM) to Air Force Manual (AFMAN) 33-145, COLLABORATION SERVICES AND VOICE SYSTEMS MANAGEMENT.

By Order of the Secretary of the Air Force, this Air Force Guidance Memorandum immediately changes Air Force Manual 33-145, *Collaboration Services And Voice Systems Management*, 6 September 2012. Compliance with this Memorandum is mandatory. To the extent its directions are inconsistent with other Air Force publications, the information herein prevails, in accordance with (IAW) AFI 33-360, *Publications and Forms Management*. Ensure that all records created as a result of processes prescribed in this publication are maintained IAW Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of IAW Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS).

As a result of the publication of AF Policy Directive(AFPD) 17-1 *Information Dominance and Cyberspace Governance and Management*, which supersedes AFPD 33-1, *Cyberspace Support*, dated 9 Aug 2012; AFMAN33-145 is hereby renumbered as AFMAN17-1202. This Memorandum also renumbers AFMAN33-145; the title and the rest of the content remain unchanged. I hereby direct the Office of Primary Responsibility (OPR) for AFMAN33-145 to conduct a special review in accordance with AFI33-360 to align its content with AFPD17-1. This will result in a rewrite or rescind action of AFMAN33-145.

This Memorandum becomes void after one year has elapsed from the date of this Memorandum, or upon rescinding or rewrite of AFMAN33-145, whichever is earlier.

WILLIAM J. BENDER, Lt Gen, USAF
Chief, Information Dominance and
Chief Information Officer

government, the subscriber pays all charges according to Title 10 U.S.C., Section 2686, Armed Forces; General Military Law, Service, Supply, and Procurement; Real Property; Related Personal Property; And Lease Of Non-Excess Property; Utilities and services: sale; expansion and extension of systems and facilities; DOD criteria; and this instruction. Offer Class B service only when an installation cannot reasonably obtain commercial service for its unofficial needs. Class B subscribers can access commercial telephone central offices and toll trunks (except where restricted). Class B service does not have direct in-dial or out-dial access to DSN and other government private line services. Class B service has the following categories:

4.10.2.1. Class B-1. Telephone lines in government-owned and government-leased quarters for family or personal use including telephone lines in unaccompanied personnel housing, visiting officers' quarters, family housing, and hospital suites.

4.10.2.2. Class B-2. Telephone lines at a military location for activities such as public schools, ARC, motion picture services, Army and Air Force Exchange Service (AAFES) services and their concessionaires, credit unions, noncommissioned officers' (NCO) and officers' open messes, youth activities (e.g., Boy Scouts and Girl Scouts), nurseries, thrift shops, commercial contractors, and other profit or non-profit organizations, service clubs, and other businesses operating on behalf of DOD, if they are on or near a DOD installation.

4.10.3. Class C. Telephone lines for transacting official government business on Air Force installations. It does not provide direct-dial access to off-base trunk lines (toll trunks, DSN). Class C lines can receive calls from off base and have access to the switchboard operator. Classes C-1 through C-4 services have the same billing categories as Class A service.

4.10.4. Class D. Telephone lines for official government business. Restrict use of these lines to special services such as fire, sentry, and crash alarms. See AFI 32-2001, *Fire Emergency Services Program*, for information on operating fire-reporting telephones.

4.11. Voice Over Internet Protocol (VoIP) Instruction. Air Force organizations considering VoIP tests or operational implementation are directed to submit an AF Form 1067 via TopVue (**https://wbgtac1p.hill.af.mil/topvue-afnic/index.aspx**). An AF Form 1067 is needed to capture VoIP capability that will be implemented at a base or for a MAJCOM if all bases within a MAJCOM are implemented using the same architecture, equipment, etc. Supporting documentation must be included identifying architectural changes to the voice system baseline, list of equipment (model), and projected cost.

4.12. Enhanced 911 (e911). Per DoDI 6055.17, *DoD Installation Emergency Management (IEM) Program,* e911 is defined as a telephone system consisting of network, database, and enhanced 911 equipment that uses the single three-digit number "911" for reporting police, fire, medical, or other emergency situations to a central location, while automatically associating a physical address with the calling party's telephone number.

4.12.1. AF installations will establish a single phone number to satisfy all A4/7 emergency response requirements (e.g. police, fire and medical) and ensure both Automatic Number Identification and Automatic Location Identification information is provided to the Emergency Communications Center (ECC).

4.12.2. Air Force installations located within the Continental United States (CONUS) with a government-owned and operated emergency dispatch are required to have e911 services with recording capability.

4.12.2.1. These CONUS installations are required to route all Emergency Service Number calls originating on the installation to the ECC.

4.12.2.2. CONUS installations receiving e911 emergency response from State and Local authorities must codify the support for these services in a Memorandum of Agreement or Understanding with the service provider.

4.12.3. Installations located Outside Continental United States (OCONUS) should provide "e911-like" services on the installation or receive similar services through agreements with the host nation.

4.12.4. Oversight for CONUS and OCONUS agreements, along with the operational use of e911, rests with the A4/7 community.

4.12.5. Technical solutions leveraging VoIP must include the capability to support e911 services. While current technology limits e911 services for cellular telephone users, future technical solutions must provide for this capability once the technology matures.

MICHAEL J. BASLA, Lt Gen, USAF
Chief, Information Dominance and
Chief Information Officer

DoD Instruction 6055.17

DoD Emergency Management (EM) Program

Originating Component:	Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics
Effective:	February 13, 2017
Releasability:	Cleared for public release. Available on the DoD Issuances Website at http://www.dtic.mil/whs/directives.
Reissues and Cancels:	DoD Instruction 6055.17, "DoD Installation Emergency Management (IEM) Program," January 13, 2009, as amended
Approved by:	James A. MacStravic, Performing the Duties of Under Secretary of Defense for Acquisition, Technology, and Logistics

Purpose: In accordance with the authority in DoD Directive (DoDD) 5134.01 and the guidance in DoDD 4715.1E, this issuance:

- Establishes policy, assigns responsibilities, and provides procedures for conducting EM activities at DoD installations worldwide.
- Establishes the DoD Emergency Management Steering Group (EMSG) to provide guidance and recommend policy on EM matters.

SECTION 5: CROSSCUTTING PREPAREDNESS CAPABILITIES: PUBLIC INFORMATION AND WARNING

5.1. INTRODUCTION. Ensuring that accurate, reliable, and actionable information on threats and hazards is available to DoD personnel and the public is critical to all aspects of preparedness and highlights the need for public information and warning capabilities to support the five preparedness mission areas—prevention, protection, mitigation, response, and recovery.

5.2. EMERGENCY COMMUNICATIONS. All EM Programs must develop a comprehensive, integrated, and interoperable emergency communications capability with an approved communications plan.

5.3. CONTINUOUS WARNING POINT. All EM Programs must designate a continuous warning point to receive and transmit emergency warning information to C3 nodes and personnel.

5.4. ENHANCED 9-1-1 (E9-1-1). Where technically feasible, all installations must have the availability of E9-1-1 services with recording capability through either government-owned and -operated support or support from civilian authorities. DoD-owned E9-1-1 systems must include the ability to receive:

a. E9-1-1 calls directly from landlines on the installation.

b. E9-1-1 calls from wireless service providers as technology matures.

c. Accurate physical location data including, as appropriate, a National Emergency Number Association-compliant street address or latitude and longitude. Latitude and longitude must be included for those cases of wireless calls coming from remote areas that are not in the vicinity of a geospatial feature such as a building polygon, street centerline, etc.

5.5. MWN.

a. DoD will pursue a single, enterprise-wide MWN system. MWN systems enable timely dissemination of alerts and warnings of hazards and threats that may impact the protected population, on and off DoD installations, allowing time for appropriate protective actions to be taken.

(1) Alert notifications requiring immediate action must be issued within 2 minutes of incident notification and verification to the affected DoD population, regardless of DoD Component affiliation, within appropriate geographic regions.

(2) Within 10 minutes after initiation, MWN systems must reach a target audience of 90 percent or more of the protected population with specific protective action recommendations

systems for communication, information management, and intelligence and information sharing across installation departments and responders.

Helps with collaborative planning and assists all echelons to achieve situational awareness.

Provides consistency at all levels of incident management across jurisdictions, as well as between various governmental jurisdictions, and with private-sector organizations and NGOs.

Should include the minimum set of geospatial features (including imagery) necessary to provide a foundational map depicting the built and natural infrastructure of a typical installation, which are of common interest or importance during emergency response events. Installation geospatial data should be obtained from the authoritative data source for each installation as defined in DoDI 8130.01.

credentialing. The authentication and verification of the training, certification, and identity of designated first responder, first receiver, and emergency responder personnel.

critical asset. Defined in the DoD Dictionary of Military and Associated Terms.

defense critical infrastructure. The composite of DoD and non-DoD assets essential to project, support, and sustain military forces and operations worldwide. It is a combination of task critical assets and defense critical assets.

DoD professional emergency manager. An individual who has the knowledge, skills, and abilities to manage a comprehensive EM Program effectively.

DoD Professional Emergency Manager Certification Program. Designates prescribed training and educational criteria plus a working knowledge of all basic tenets of EM throughout mitigation, preparedness, response, and recovery.

DSCA. Defined in DoDD 3025.18.

E9-1-1 capability. A telecommunications system consisting of networks, databases, and E9-1-1 equipment that uses the single three-digit number "9-1-1" for reporting police, fire, medical, and other emergency situations to a central location, while automatically associating a physical location and calling party's telephone number. The physical location is correlated with the applicable emergency service number to route E9-1-1 calls to the correct public safety answering point for servicing by the corresponding emergency service agency.

ECC. A tailored mix of facilities, equipment, personnel, and procedures to:

Provide emergency call-taking for emergency and non-emergency calls for service.

Provide dispatch services for first responders, first receivers, and emergency responders.

Provide emergency communications capabilities.

Maintain records of all communications and activities.

Appendix E.
El Paso-Teller County Intergovernmental Agreement

EL PASO - TELLER COUNTY
EMERGENCY TELEPHONE SERVICE AUTHORITY

SECOND AMENDED AND RESTATED INTERGOVERNMENTAL AGREEMENT

THIS SECOND AMENDED AND RESTATED INTERGOVERNMENTAL AGREEMENT (the "Second Restated IGA") is made and entered into by and among the governmental entities who sign this Agreement (individually referred to herein as a "Party" and collectively as the "Parties"). This Second Restated IGA amends and restates in its entirety that Restated Intergovernmental Agreement of 2000 (the "First Restated IGA"), by and among certain governmental entities, and becomes effective when signed by three-fourths (3/4) of the parties to the First Restated IGA, as further described herein.

RECITALS

1. WHEREAS, pursuant to Article 11 of Title 29, Colorado Revised Statutes (the "Emergency Telephone Service Law"), the Parties have the power to enter into agreements for the purpose of providing emergency telephone and notification services, and imposing an emergency telephone charge for such services; and

2. WHEREAS, the Emergency Telephone Service Law authorizes such legal entities to undertake various actions in connection with providing such services, including the right to impose an emergency telephone charge on each exchange access, wireless communications access, and interconnected voice-over-internet-protocol communications access within the service area of the Parties; and

3. WHEREAS, Part 2 of Article 1 of Title 29, Colorado Revised Statutes (the "Intergovernmental Relations Law"), as amended, encourages and authorizes governmental entities to enter into intergovernmental agreements of this nature, and Section 29-1-203.5, C.R.S. authorizes the establishment of a legal entity that is a separate political subdivision and public corporation to carry out the purposes of the Intergovernmental Relations Law and the Emergency Telephone Service Law; and

4. WHEREAS, it would serve the public welfare and be in the best interest of the Parties to continue, through an intergovernmental agreement, a central emergency telephone service authority, and provide for its organization, administration, and operation; and

5. WHEREAS, in 1989 multiple governmental entities entered into an Intergovernmental Agreement (the "1989 IGA") to implement the provisions of the Emergency Telephone Service Law by establishing the El Paso - Teller County Emergency Telephone Service Authority (the "Authority"). In 2000, the 1989 IGA was amended and restated pursuant to the First Restated IGA. In 2002, the First Amendment

of Restated IGA was approved to clarify the 911 Authority's power regarding property, to facilitate financing and construction of the 911 Authority building on Airport Road. The purpose of the Authority upon organization was, and still remains, to impose the emergency telephone service charge, to incur costs associated with operation of the emergency telephone service and emergency notification service, and to administer the operation of the emergency telephone and emergency notification services.

6. WHEREAS, Section VIII of the First Restated IGA provides that it may be amended by a writing executed by at least three-fourths (3/4) of the parties to the First Restated IGA. Based on the original parties to the First Restated IGA, less those entities that signed the First Restated IGA but are no longer in existence and plus those entities that signed the First Restated IGA subsequent to the effective date thereof, the Parties acknowledge and agree that there are thirty (30) parties to the First Restated IGA. The Parties further agree that to amend the First Restated IGA and have this Second Restated IGA become effective requires the signatures of at least twenty-three (23) of the entities listed on the signature pages at the end of this Second Restated IGA, which represents at least three-fourths of the parties to the First Restated IGA.

7. WHEREAS, the Parties have determined that it is appropriate and necessary to amend and restate the First Restated IGA in its entirety to properly reflect changes in the law and to make changes in the organization, administration and operation of the Authority.

8. WHEREAS, the Parties desire to enter into this Second Restated IGA for the following purposes:

1) To continue the existence of the Authority as a separate political subdivision and public corporation organized pursuant to Section 29-1-203.5, C.R.S. The Authority is the legal entity responsible for carrying out the purposes of the Emergency Telephone Service Law and administering and operating the emergency telephone and notification systems within the Parties' service area; and

2) To define the manner in which each of the Parties will participate in the Authority.

NOW, THEREFORE, in consideration of the recitals above and the mutual covenants hereinafter set forth, the Parties amend and restate in full the First Restated IGA and agree as follows:

I. General Provisions.

The recitals contained above are incorporated and agreed to as if set forth here in full. The Parties hereby continue the existence of the Authority, which is responsible for administering the operation of the emergency telephone and notification services within

El Paso and Teller Counties. The Authority may also be referred to as the "El Paso-Teller County 9-1-1 Authority." The operation of the Authority shall be as is set forth herein and in the Bylaws, Rules, Regulations and Policies of the Authority adopted pursuant to Section IV below.

II. Parties to this Agreement.

The Parties to this Agreement are those governmental entities which sign this Agreement. They may consist of all or some of the following: El Paso and Teller Counties, the cities, towns, military installations, and special districts (including ambulance districts, fire protection districts, health service districts, hospital districts, metropolitan districts, regional service authorities, and law enforcement authorities) within said counties, and other governmental entities in El Paso and Teller Counties, which are primary providers of emergency firefighting, law enforcement, ambulance, emergency medical or other emergency services who receive services from the Authority. Any future city, town, military installation or special district, after having been legally formed and meeting the foregoing criteria, may make a written request to the Board of Directors of the Authority (the "Board") to become a signatory to this Agreement, and upon Board approval shall become a party hereto effective on January 1 of the year following signing.

III. Board of Directors.

The Authority shall be governed by a Board of Directors consisting of nine (9) members to be selected in the following manner:

A. Cities, Towns, U.S. Military, and Special Districts Other Than Appointing Authorities.

The Board shall appoint three (3) members to the Board from a list of nominees submitted by any of the Parties, other than the Appointing Authorities listed below. Such Board members must be residents of El Paso or Teller County.

Nothing in this section shall preclude the Parties, other than the Appointing Authorities, from determining by a majority vote, their choice(s) for appointment. Upon written notice of the selection(s), the Board shall make the appointment(s).

B. Appointing Authorities.

The Board of County Commissioners of El Paso County shall appoint two (2) members of the Board, who must be residents of either El Paso or Teller County.

The Board of County Commissioners of Teller County shall appoint one (1) member of the Board, who must be a resident of either El Paso or Teller County.

The City Council of the City of Colorado Springs shall appoint three (3) members of the

Board, who must be residents of either El Paso or Teller County.

C. Terms of Appointment.

Members of the Board are eligible to serve consecutive terms on the Board, but no member shall serve for more than two (2) consecutive terms. Each term shall be for a period of three (3) years.

A member of the Board who is absent from three successive regular or work session meetings of the Board, without being excused, shall be disqualified from continuing to serve as a Director, and his or her term shall terminate on the date of the third consecutive unexcused absence. The Board may establish rules and procedures for excusing Board members from meetings and work sessions.

D. Existing Members of the Authority Board.

All members of the Board of the Authority who have been duly appointed and are serving pursuant to the provisions of the First Restated IGA shall continue to serve in such capacity, and for the term for which they were appointed.

IV. Rules and Regulations.

The Board may adopt Bylaws, Rules, Regulations, and Policies so long as they do not conflict with the Emergency Telephone Service Law or the Intergovernmental Relations Law, the provisions of this Second Restated IGA, or provisions of other laws of the State of Colorado applicable to the Authority.

V. Powers of the Authority.

The Authority, through its Board, is empowered and authorized to carry out the Emergency Telephone Service Law, including but not limited to:

A. To set, impose, receive, and collect an emergency telephone charge for the provision of continued and adequate emergency telephone service and emergency notification service within all areas of El Paso and Teller Counties, pursuant to and subject to the limits set by §29-11-102, C.R.S.;

B. To receive remittances of prepaid wireless E911 charges pursuant to §29-11-102.5, C.R.S.;

C. To take legal action pursuant to §29-11-102(6), C.R.S. to enforce the collection of any emergency telephone charges which are unpaid within El Paso and Teller Counties;

D. To contract for the installation and operation of an emergency telephone service, an emergency notification service and any other services to the extent permitted by the Emergency Telephone Service Law;

E. To enter into contracts for emergency telephone service with a BESP, as defined in §29-11-101(1.2), C.R.S., and spend emergency telephone charges and prepaid wireless E911 charges as provided in §29-11-102(1) and §29-11-104, C.R.S.;

F. To perform all of the above actions directly or by contract, and on behalf of any or all Parties; and

G. Perform any other act in connection with provision of emergency telephone service, emergency notification service and any other services permitted by law.

VI. Limitations on Authority Powers and Parties' Use of Authority Funds.

The Authority may not impose a fee, charge, or financial obligation on any Party without that Party's consent; however, this does not prohibit the Board from imposing requirements or conditions on receiving assistance or funding from the Authority. The Parties agree that any funds, services and assets made available by the Authority to any Party which are funded from revenues generated by the emergency telephone service charge imposed pursuant to §§29-11-102 and 29-11-102.5, C.R.S. will only be used in a manner consistent with §§29-11-100.5, et seq., C.R.S. Each Party further agrees to use any such funds, services and assets subject to any express written conditions of approval specified by the Authority Board of Directors, written policies in effect at the time of approval, and any written agreements entered into between the Authority and such Party.

VII. Annual Report.

After the completion of its annual audit, the Authority shall prepare and present to the Parties, a comprehensive Annual Report of the Authority's activities and finances during the preceding year.

VIII. Term and Termination.

This Second Restated IGA shall become effective upon execution by at least twenty-three (23) of the entities listed on the signature pages at the end of this Second Restated IGA, which represents at least three-fourths (3/4) of the parties to the First Restated IGA, as further described in the Recitals. This Second Restated IGA shall continue in full force and effect, subject to amendments, or until sooner terminated by a writing signed by at least three-fourths (3/4) of the Parties who directly operate a public safety answering point, as defined in §29-11-101(6.5), C.R.S.

Upon the termination of this Second Restated IGA the powers granted to the Authority, and exercised by its Board shall continue to the extent necessary to make an effective disposition of the assets of the Authority, and for the payment of any obligations of the Authority. All assets purchased with Authority funds and placed with a Party shall be transferred to such Party. All assets of the Authority held by the Authority for the common benefit of the Parties shall be disposed of and the proceeds distributed to the Parties which, as of the termination, will continue to operate a public safety answering point, in proportion to the number of emergency 911 calls received by such Parties for the calendar year prior to termination.

IX. Withdrawal of a Party.

The participation of a Party or Parties in this Second Restated IGA may be withdrawn by written notice from the Party or Parties to the Authority at least one hundred eighty (180) days prior to January 1 of any given year. Upon withdrawal of the participation of a Party or Parties pursuant to this provision or for any other cause (other than by a termination of the Second Restated IGA), such Party or Parties shall forfeit all right, title, and interest in and to any assets of the Authority.

In the event any Party to this Second Restated IGA is dissolved or ceases to be a legal entity, such entity shall cease to be a Party on the date its legal status is changed, and such Party shall have no further right, title, or interest in any of the assets of the Authority.

X. Amendments to this Second Restated IGA.

This Second Restated IGA may be amended by the Parties from time to time, but any amendment shall be in writing and signed by at least three-fourths (3/4) of the Parties who directly operate a public safety answering point, as defined in §29-11-101(6.5), C.R.S.

XI. Liability of Directors.

The members of the Board, and its officers, shall not be personally liable for any acts performed or omitted in good faith. The Authority shall indemnify, defend, and hold harmless any member of the Board, officer and employee from and against claims or judgments of third parties, resulting from the acts or omissions of such person occurring during the performance of his duties and within the scope of his employment, except where such act or omission is willful and wanton. The Board may purchase insurance to provide liability and other coverages, as is deemed necessary or appropriate by the Board, for the Authority, the members of its Board, its officers and employees.

The Authority may obtain a bond or other security to guarantee the faithful performance of the duties of the Board and its officers.

The Parties, by executing this Second Restated IGA, do not waive any or all of the immunities, protections, rights, procedures, and limitations provided under the Colorado Governmental Immunity Act, §24-10-101 *et seq.*, C.R.S., or any other law.

XII. Severability Clause.

If any provision of this Second Restated IGA or the application hereof to any Party or circumstances is held invalid, such invalidity shall not affect other provisions or applications of this Second Restated IGA which can be given effect without the invalid provision or application, and to this end the provisions of this Second Restated IGA are declared to be severable.

XIII. Execution in Counterparts

This Second Restated IGA may be signed by each Party separately, each of which shall be an original, but all of which, taken together, shall be deemed a full and complete agreement.

IN WITNESS WHEREOF, the Parties have caused their duly authorized representatives to sign this Second Restated IGA, and to affix their seal hereon, on the dates set forth below.

APPOINTING AUTHORITIES:

COUNTY OF EL PASO

Signature: _____

Title/Position: _____

Date: _____

COUNTY OF TELLER

Signature: _____

Title/Position: _____

Date: _____

CITY OF COLORADO SPRINGS

Signature: _____

Title/Position: _____

Date: _____

The Parties, by executing this Second Restated IGA, do not waive any or all of the immunities, protections, rights, procedures, and limitations provided under the Colorado Governmental Immunity Act, §24-10-101 *et seq.*, C.R.S., or any other law.

XII. Severability Clause.

If any provision of this Second Restated IGA or the application hereof to any Party or circumstances is held invalid, such invalidity shall not affect other provisions or applications of this Second Restated IGA which can be given effect without the invalid provision or application, and to this end the provisions of this Second Restated IGA are declared to be severable.

XIII. Execution in Counterparts

This Second Restated IGA may be signed by each Party separately, each of which shall be an original, but all of which, taken together, shall be deemed a full and complete agreement.

IN WITNESS WHEREOF, the Parties have caused their duly authorized representatives to sign this Second Restated IGA, and to affix their seal hereon, on the dates set forth below.

APPOINTING AUTHORITIES:

COUNTY OF EL PASO

Signature: _____
17-221

Title/Position: President

Date: 8/1/2017

COUNTY OF TELLER

Signature: _____

Title/Position: _____

Date: _____

CITY OF COLORADO SPRINGS

Signature: _____

Title/Position: _____

Date: _____

The Parties, by executing this Second Restated IGA, do not waive any or all of the immunities, protections, rights, procedures, and limitations provided under the Colorado Governmental Immunity Act, §24-10-101 *et seq.*, C.R.S., or any other law.

XII. Severability Clause.

If any provision of this Second Restated IGA or the application hereof to any Party or circumstances is held invalid, such invalidity shall not affect other provisions or applications of this Second Restated IGA which can be given effect without the invalid provision or application, and to this end the provisions of this Second Restated IGA are declared to be severable.

XIII. Execution in Counterparts

This Second Restated IGA may be signed by each Party separately, each of which shall be an original, but all of which, taken together, shall be deemed a full and complete agreement.

IN WITNESS WHEREOF, the Parties have caused their duly authorized representatives to sign this Second Restated IGA, and to affix their seal hereon, on the dates set forth below.

APPOINTING AUTHORITIES:

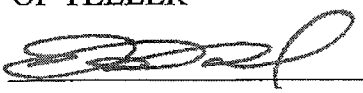
COUNTY OF EL PASO

Signature: _____

Title/Position: _____

Date: _____

COUNTY OF TELLER

Signature: 

Title/Position: Chairman

Date: September 28, 2017

CITY OF COLORADO SPRINGS

Signature: _____

Title/Position: _____

Date: _____

The Parties, by executing this Second Restated IGA, do not waive any or all of the immunities, protections, rights, procedures, and limitations provided under the Colorado Governmental Immunity Act, §24-10-101 *et seq.*, C.R.S., or any other law.

XII. Severability Clause.

If any provision of this Second Restated IGA or the application hereof to any Party or circumstances is held invalid, such invalidity shall not affect other provisions or applications of this Second Restated IGA which can be given effect without the invalid provision or application, and to this end the provisions of this Second Restated IGA are declared to be severable.

XIII. Execution in Counterparts

This Second Restated IGA may be signed by each Party separately, each of which shall be an original, but all of which, taken together, shall be deemed a full and complete agreement.

IN WITNESS WHEREOF, the Parties have caused their duly authorized representatives to sign this Second Restated IGA, and to affix their seal hereon, on the dates set forth below.

APPOINTING AUTHORITIES:

COUNTY OF EL PASO

Signature: _____

Title/Position: _____

Date: _____

COUNTY OF TELLER

Signature: _____

Title/Position: _____

Date: _____

CITY OF COLORADO SPRINGS

Signature: _____

Title/Position: Mayor

Date: 3/23/2018

APPROVED AS TO FORM
CITY OF COLORADO SPRINGS
CITY ATTORNEY'S OFFICE

Name: Frederick Stein

CITIES, TOWNS, MILITARY INSTALLATIONS AND SPECIAL DISTRICTS:

CITY OF CRIPPLE CREEK

Signature: _____

Title/Position: Mayor

Date: 9-6-17

CITY OF FOUNTAIN

Signature: _____

Title/Position: _____

Date: _____

CITY OF MANITOU SPRINGS

Signature: _____

Title/Position: _____

Date: _____

CITY OF VICTOR

Signature: _____

Title/Position: _____

Date: _____

CITY OF WOODLAND PARK

Signature: _____

Title/Position: _____

Date: _____

TOWN OF CALHAN

Signature: _____

Title/Position: _____

Date: _____

TOWN OF GREEN MOUNTAIN FALLS

Signature: _____

Title/Position: _____

Date: _____

TOWN OF MONUMENT

Signature: _____

Title/Position: _____

Date: _____

CITIES, TOWNS, MILITARY INSTALLATIONS AND SPECIAL DISTRICTS:

CITY OF CRIPPLE CREEK

Signature: _____

Title/Position: _____

Date: _____

CITY OF FOUNTAIN

Signature: Fred P. Ortega

Title/Position: Mayor

Date: 10/10/2017

CITY OF MANITOU SPRINGS

Signature: _____

Title/Position: _____

Date: _____

CITY OF VICTOR

Signature: _____

Title/Position: _____

Date: _____

CITY OF WOODLAND PARK

Signature: _____

Title/Position: _____

Date: _____

TOWN OF CALHAN

Signature: _____

Title/Position: _____

Date: _____

TOWN OF GREEN MOUNTAIN FALLS

Signature: _____

Title/Position: _____

Date: _____

TOWN OF MONUMENT

Signature: _____

Title/Position: _____

Date: _____

CITIES, TOWNS, MILITARY INSTALLATIONS AND SPECIAL DISTRICTS:

CITY OF CRIPPLE CREEK

Signature: _____

Title/Position: _____

Date: _____

CITY OF FOUNTAIN

Signature: _____

Title/Position: _____

Date: _____

CITY OF MANITOU SPRINGS

Signature: Nicole Nicoletti

Title/Position: Mayor

Date: June 13, 2017

CITY OF VICTOR

Signature: _____

Title/Position: _____

Date: _____

CITY OF WOODLAND PARK

Signature: _____

Title/Position: _____

Date: _____

TOWN OF CALHAN

Signature: _____

Title/Position: _____

Date: _____

TOWN OF GREEN MOUNTAIN FALLS

Signature: _____

Title/Position: _____

Date: _____

TOWN OF MONUMENT

Signature: _____

Title/Position: _____

Date: _____

CITIES, TOWNS, MILITARY INSTALLATIONS AND SPECIAL DISTRICTS:

CITY OF CRIPPLE CREEK

Signature: _____

Title/Position: _____

Date: _____

CITY OF FOUNTAIN

Signature: _____

Title/Position: _____

Date: _____

CITY OF MANITOU SPRINGS

Signature: _____

Title/Position: _____

Date: _____

CITY OF VICTOR

Signature: Byron L. Idaberg Jr.

Title/Position: Mayor

Date: 6/15/17

CITY OF WOODLAND PARK

Signature: _____

Title/Position: _____

Date: _____

TOWN OF CALHAN

Signature: _____

Title/Position: _____

Date: _____

TOWN OF GREEN MOUNTAIN FALLS

Signature: _____

Title/Position: _____

Date: _____

TOWN OF MONUMENT

Signature: _____

Title/Position: _____

Date: _____

CITIES, TOWNS, MILITARY INSTALLATIONS AND SPECIAL DISTRICTS:

CITY OF CRIPPLE CREEK

Signature: _____

Title/Position: _____

Date: _____

CITY OF FOUNTAIN

Signature: _____

Title/Position: _____

Date: _____

CITY OF MANITOU SPRINGS

Signature: _____

Title/Position: _____

Date: _____

CITY OF VICTOR

Signature: _____

Title/Position: _____

Date: _____

CITY OF WOODLAND PARK

Signature: [signature]

Title/Position: Mayor of Woodland Park

Date: November 2, 2017

TOWN OF CALHAN

Signature: _____

Title/Position: _____

Date: _____

TOWN OF GREEN MOUNTAIN FALLS

Signature: _____

Title/Position: _____

Date: _____

TOWN OF MONUMENT

Signature: _____

Title/Position: _____

Date: _____

CITIES, TOWNS, MILITARY INSTALLATIONS AND SPECIAL DISTRICTS:

CITY OF CRIPPLE CREEK

Signature: _____

Title/Position: _____

Date: _____

CITY OF FOUNTAIN

Signature: _____

Title/Position: _____

Date: _____

CITY OF MANITOU SPRINGS

Signature: _____

Title/Position: _____

Date: _____

CITY OF VICTOR

Signature: _____

Title/Position: _____

Date: _____

CITY OF WOODLAND PARK

Signature: _____

Title/Position: _____

Date: _____

TOWN OF CALHAN

Signature: _____

Title/Position: Mayor

Date: 6/12/17

TOWN OF GREEN MOUNTAIN FALLS

Signature: _____

Title/Position: _____

Date: _____

TOWN OF MONUMENT

Signature: _____

Title/Position: _____

Date: _____

CITIES, TOWNS, MILITARY INSTALLATIONS AND SPECIAL DISTRICTS:

CITY OF CRIPPLE CREEK

Signature: _____

Title/Position: _____

Date: _____

CITY OF FOUNTAIN

Signature: _____

Title/Position: _____

Date: _____

CITY OF MANITOU SPRINGS

Signature: _____

Title/Position: _____

Date: _____

CITY OF VICTOR

Signature: _____

Title/Position: _____

Date: _____

CITY OF WOODLAND PARK

Signature: _____

Title/Position: _____

Date: _____

TOWN OF CALHAN

Signature: _____

Title/Position: _____

Date: _____

TOWN OF GREEN MOUNTAIN FALLS

Signature: Kate L Bruce

Title/Position: Town Manager

Date: 10-18-2017

TOWN OF MONUMENT

Signature: _____

Title/Position: _____

Date: _____

CITIES, TOWNS, MILITARY INSTALLATIONS AND SPECIAL DISTRICTS:

CITY OF CRIPPLE CREEK

Signature: _____

Title/Position: _____

Date: _____

CITY OF FOUNTAIN

Signature: _____

Title/Position: _____

Date: _____

CITY OF MANITOU SPRINGS

Signature: _____

Title/Position: _____

Date: _____

CITY OF VICTOR

Signature: _____

Title/Position: _____

Date: _____

CITY OF WOODLAND PARK

Signature: _____

Title/Position: _____

Date: _____

TOWN OF CALHAN

Signature: _____

Title/Position: _____

Date: _____

TOWN OF GREEN MOUNTAIN FALLS

Signature: _____

Title/Position: _____

Date: _____

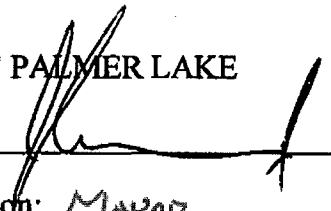
TOWN OF MONUMENT

Signature: [signature]

Title/Position: Mayor Pro Tem

Date: 11/20/17

TOWN OF PALMER LAKE

Signature: 

Title/Position: Mayor

Date: 2-8-18

TOWN OF RAMAH

Signature: _____

Title/Position: _____

Date: _____

BIG SANDY FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

BLACK FOREST FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

BROADMOOR FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

CALHAN FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

CASCADE FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

CIMARRON FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

TOWN OF PALMER LAKE

Signature: _____

Title/Position: _____

Date: _____

TOWN OF RAMAH

Signature: Dennis Hinton

Title/Position: Mayor

Date: 6-12-17

BIG SANDY FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

BLACK FOREST FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

BROADMOOR FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

CALHAN FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

CASCADE FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

CIMARRON FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

TOWN OF PALMER LAKE

Signature: _____

Title/Position: _____

Date: _____

TOWN OF RAMAH

Signature: _____

Title/Position: _____

Date: _____

BIG SANDY FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

BLACK FOREST FIRE PROTECTION DISTRICT

Signature: [signature]

Title/Position: Fire Chief

Date: 2/14/18

BROADMOOR FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

CALHAN FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

CASCADE FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

CIMARRON FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

TOWN OF PALMER LAKE

Signature: _____

Title/Position: _____

Date: _____

TOWN OF RAMAH

Signature: _____

Title/Position: _____

Date: _____

BIG SANDY FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

BLACK FOREST FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

BROADMOOR FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: Chief

Date: 7/29/17

CALHAN FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

CASCADE FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

CIMARRON FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

TOWN OF PALMER LAKE

Signature: _____

Title/Position: _____

Date: _____

TOWN OF RAMAH

Signature: _____

Title/Position: _____

Date: _____

BIG SANDY FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

BLACK FOREST FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

BROADMOOR FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

CALHAN FIRE PROTECTION DISTRICT

Signature: Albert Kobulan

Title/Position: Chair

Date: 3-8-2018

CASCADE FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

CIMARRON FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

TOWN OF PALMER LAKE

Signature: _____

Title/Position: _____

Date: _____

TOWN OF RAMAH

Signature: _____

Title/Position: _____

Date: _____

BIG SANDY FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

BLACK FOREST FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

BROADMOOR FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

CALHAN FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

CASCADE FIRE PROTECTION DISTRICT

Signature: Robert Littrell

Title/Position: Board President

Date: Aug. 14, 2017

CIMARRON FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

TOWN OF PALMER LAKE

Signature: _____

Title/Position: _____

Date: _____

TOWN OF RAMAH

Signature: _____

Title/Position: _____

Date: _____

BIG SANDY FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

BLACK FOREST FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

BROADMOOR FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

CALHAN FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

CASCADE FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

CIMARRON FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: Fire Chief

Date: 10/16/17

COLORADO CENTRE METROPOLITAN DISTRICT

Signature: _____

Title/Position: _____

Date: _____

DIVIDE FIRE PROTECTION DISTRICT

Signature: J. W. Clinkenbeard

Title/Position: President of the Board

Date: 4/13/17

DONALD WESCOTT FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

ELBERT FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

EDISON FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

ELLICOTT FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

FALCON FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

FLORISSANT FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

COLORADO CENTRE METROPOLITAN DISTRICT

Signature: _____

Title/Position: _____

Date: _____

DIVIDE FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

DONALD WESCOTT FIRE PROTECTION DISTRICT

Signature: [signature]

Title/Position: FIRE CHIEF

Date: 2-22-2018

ELBERT FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

EDISON FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

ELLICOTT FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

FALCON FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

FLORISSANT FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

COLORADO CENTRE METROPOLITAN DISTRICT

Signature: _____

Title/Position: _____

Date: _____

DIVIDE FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

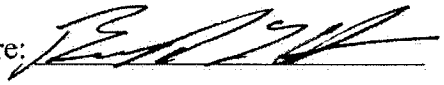
DONALD WESCOTT FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

ELBERT FIRE PROTECTION DISTRICT

Signature: 

Title/Position: Fire Chief

Date: 6-3-17

EDISON FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

ELLICOTT FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

FALCON FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

FLORISSANT FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

COLORADO CENTRE METROPOLITAN DISTRICT

Signature: _____

Title/Position: _____

Date: _____

DIVIDE FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

DONALD WESCOTT FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

ELBERT FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

EDISON FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

ELLICOTT FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

FALCON FIRE PROTECTION DISTRICT

Signature: [signature]

Title/Position: Fire Chief

Date: 7/12/2017

FLORISSANT FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

Date: _____

Date: _____

DONALD WESCOTT FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

ELBERT FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

EDISON FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

ELLICOTT FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

FALCON FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

FLORISSANT FIRE PROTECTION DISTRICT

Signature: Edward J Blecha

Title/Position: District President

Date: February 22, 2018

FOUR MILE FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

GREEN MOUNTAIN FALLS – CHIPITA PARK FIRE PROTECTIC DISTRICT

Signature: _____

Title/Position: _____

Date: _____

HANOVER FIRE PROTECTION DISTRICT

Signature:

MOUNTAIN COMMUNITIES FIRI PROTECTION DISTRICT

Signature:

FOUR MILE FIRE PROTECTION DISTRICT

Signature: 

Title/Position: TREASURER

Date: 10/5/2017

GREEN MOUNTAIN FALLS – CHIPITA PARK FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

HANOVER FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

MOUNTAIN COMMUNITIES FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

NORTHEAST TELLER COUNTY FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

PEYTON FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

SECURITY FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

SOUTHWEST HIGHWAY 115 FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

FOUR MILE FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

GREEN MOUNTAIN FALLS – CHIPITA PARK FIRE PROTECTION DISTRICT

Signature: Richard K Brown

Title/Position: Board Pres

Date: 9-14-12

HANOVER FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

MOUNTAIN COMMUNITIES FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

NORTHEAST TELLER COUNTY FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

PEYTON FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

SECURITY FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

SOUTHWEST HIGHWAY 115 FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

FOUR MILE FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

GREEN MOUNTAIN FALLS – CHIPITA PARK FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

HANOVER FIRE PROTECTION DISTRICT

Signature: [signature]

Title/Position: District Administrator

Date: 30 OCT 17

MOUNTAIN COMMUNITIES FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

NORTHEAST TELLER COUNTY FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

PEYTON FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

SECURITY FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

SOUTHWEST HIGHWAY 115 FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

FOUR MILE FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

GREEN MOUNTAIN FALLS – CHIPITA PARK FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

HANOVER FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

MOUNTAIN COMMUNITIES FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

NORTHEAST TELLER COUNTY FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: Fire Chief

Date: 6-12-2017

PEYTON FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

SECURITY FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

SOUTHWEST HIGHWAY 115 FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

FOUR MILE FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

GREEN MOUNTAIN FALLS – CHIPITA PARK FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

HANOVER FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

MOUNTAIN COMMUNITIES FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

NORTHEAST TELLER COUNTY FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

PEYTON FIRE PROTECTION DISTRICT

Signature: Patrick V. DeLaney

Title/Position: BOARD PRESIDENT

Date: December 12, 2017

SECURITY FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

SOUTHWEST HIGHWAY 115 FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

FOUR MILE FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

GREEN MOUNTAIN FALLS – CHIPITA PARK FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

HANOVER FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

MOUNTAIN COMMUNITIES FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

NORTHEAST TELLER COUNTY FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

PEYTON FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

SECURITY FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: Fire Chief

Date: 10-19-17

SOUTHWEST HIGHWAY 115 FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

FOUR MILE FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

GREEN MOUNTAIN FALLS – CHIPITA PARK FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

HANOVER FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

MOUNTAIN COMMUNITIES FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

NORTHEAST TELLER COUNTY FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

PEYTON FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

SECURITY FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

SOUTHWEST HIGHWAY 115 FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: Board President

Date: 5-24-17

SOUTHERN TELLER COUNTY HEALTH SERVICES DISTRICT

Signature: _____

Title/Position: _____

Date: _____

STRATMOOR HILLS FIRE PROTECTION DISTRICT

Signature: Dianne M Cooper

Title/Position: Board Chairperson

Date: 2/21/18

TRI-COUNTY FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

TRI-LAKES MONUMENT FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

UTE PASS REGIONAL HEALTH SERVICE DISTRICT

Signature: _____

Title/Position: _____

Date: _____

FORT CARSON ARMY POST

Signature: _____

Title/Position: _____

Date: _____

PETERSON AIR FORCE BASE

Signature: _____

Title/Position: _____

Date: _____

U.S. AIR FORCE ACADEMY

Signature: _____

Title/Position: _____

Date: _____

SOUTHERN TELLER COUNTY HEALTH SERVICES DISTRICT

Signature: _____

Title/Position: _____

Date: _____

STRATMOOR HILLS FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

TRI-COUNTY FIRE PROTECTION DISTRICT

Signature: _____

Title/Position: _____

Date: _____

TRI-LAKES MONUMENT FIRE PROTECTION DISTRICT

Signature: [signature]

Title/Position: FIRE CHIEF

Date: 7/31/17

UTE PASS REGIONAL HEALTH SERVICE DISTRICT

Signature: _____

Title/Position: _____

Date: _____

FORT CARSON ARMY POST

Signature: _____

Title/Position: _____

Date: _____

PETERSON AIR FORCE BASE

Signature: _____

Title/Position: _____

Date: _____

U.S. AIR FORCE ACADEMY

Signature: _____

Title/Position: _____

Date: _____

Appendix F.
Virginia Beach Regional ESInet RFP

REQUEST FOR PROPOSAL

City of Virginia Beach
ISSUING OFFICE:
PURCHASING DIVISION
2388 LIBERTY WAY
VIRGINIA BEACH, VA 23456
TELEPHONE: (757) 385-4438 FAX: (757) 385-5601

DATE: January 4, 2019
Attention of Offeror is Directed To Section 2.2-4367 – 2.2-4377 of Virginia Public Procurement Act ("VPPA") **(Ethics In Public Contracting)**

RFP ITEM NO. **ITAS-16-0065**
CLOSING DATE **FEBRUARY 6, 2019**
CLOSING TIME **3:00 PM EST**
PROCUREMENT OFFICER **Darla Smith**

PLEASE FILL IN COMPANY NAME & ADDRESS IN THE SPACES PROVIDED BELOW:

_____

_____

_____

RETURN THIS COPY

THIS IS NOT AN ORDER

THE City RESERVES THE RIGHT TO ACCEPT OR REJECT ANY AND ALL PROPOSALS IN WHOLE OR IN PART AND WAIVE ANY INFORMALITIES IN THE COMPETITIVE NEGOTIATION PROCESS. FURTHER, THE CITY RESERVES THE RIGHT TO ENTER INTO ANY CONTRACT DEEMED TO BE IN THE BEST INTEREST OF THE CITY.

DESCRIPTION OF REQUEST FOR PROPOSAL

THIS DOCUMENT CONSTITUTES A REQUEST FOR SEALED PROPOSALS FROM QUALIFIED INDIVIDUALS AND/OR ORGANIZATIONS TO PROVIDE EMERGENCY SERVICES INTERNET PROTOCAL NETWORK SERVICES (ESInet) AND SUPPORTING NEXT GENERATION CORE SERVICES ("NGCS") WHICH ARE NENA i3 COMPLIANT FOR THE City.

A **pre-proposal conference** will be held in the Purchasing Division's conference room located at 2388 Liberty Way Drive, Virginia Beach, Virginia 23456. The conference will be held at 11:30 **EST a.m. on Friday, January 18, 2019**. A phone bridge has been setup for telephone attendance. Interested participants may call in at (757) 385-1785 (local number) and 1-(877) 222-2238 (long distance number). Access Meeting ID 5940.

The Virginia Beach City Council has adopted a 10% goal for minority participation in City Contracts.

ACKNOWLEDGE RECEIPT OF ADDENDUM: #1____ #2____ #3____ #4____ (Please Initial)

IN COMPLIANCE WITH THIS SOLICITATION AND TO ALL THE CONDITIONS IMPOSED HEREIN, THE UNDERSIGNED AGREES TO EXECUTE THE CONTRACT AS A RESULT OF THIS SOLICITATION. AN AGENT AUTHORIZED TO BIND THE COMPANY SHALL SIGN THE FOLLOWING SECTION. FAILURE TO EXECUTE THIS PORTION MAY RESULT IN PROPOSAL REJECTION.

AUTHORIZED AGENT/SIGNATURE_____ TELEPHONE:_____

TYPE OR PRINT NAME:_____DATE: _____

ENCLOSURE

ANTICOLLUSION/NONDISCRIMINATION/DRUG-FREE WORKPLACE CLAUSE

ANTICOLLUSION CLAUSE:
IN THE PREPARATION AND SUBMISSION OF THIS BID, SAID OFFEROR DID NOT EITHER DIRECTLY OR INDIRECTLY ENTER INTO ANY COMBINATION OR ARRANGEMENT WITH ANY PERSON, FIRM OR CORPORATION, OR ENTER INTO ANY AGREEMENT, PARTICIPATE IN ANY COLLUSION, OR OTHERWISE TAKE ANY ACTION IN THE RESTRAINT OF FREE, COMPETITIVE BIDDING IN VIOLATION OF THE SHERMAN ACT (15 U.S.C. SECTION 1), SECTIONS 59.1-9.1 THROUGH 59.1-9.17 OR SECTIONS 59.1-68.8 THROUGH 59.1-68.8 OF THE CODE OF VIRGINIA.

THE UNDERSIGNED OFFEROR HEREBY CERTIFIES THAT THIS AGREEMENT, OR ANY CLAIMS RESULTING THERE FROM, IS NOT THE RESULT OF, OR AFFECTED BY, ANY ACT OF COLLUSION WITH, OR ANY ACT OF, ANOTHER PERSON OR PERSONS, FIRM OR CORPORATION ENGAGED IN THE SAME LINE OF BUSINESS OR COMMERCE; AND, THAT NO PERSON ACTING FOR, OR EMPLOYED BY, THE City HAS AN INTEREST IN, OR IS CONCERNED WITH, THIS BID; AND, THAT NO PERSON OR PERSONS, FIRM OR CORPORATION OTHER THAN THE UNDERSIGNED, HAVE, OR ARE, INTERESTED IN THIS BID.

DRUG-FREE WORKPLACE:
DURING THE PERFORMANCE OF THIS CONTRACT, THE CONTRACTOR AGREES TO (I) PROVIDE A DRUG-FREE WORKPLACE FOR THE CONTRACTOR'S EMPLOYEES; (II) POST IN CONSPICUOUS PLACES, AVAILABLE TO EMPLOYEES AND APPLICANTS FOR EMPLOYMENT, A STATEMENT NOTIFYING EMPLOYEES THAT THE UNLAWFUL MANUFACTURE, SALE, DISTRIBUTION, DISPENSATION, POSSESSION, OR USE OF A CONTROLLED SUBSTANCE OR MARIJUANA IS PROHIBITED IN THE CONTRACTOR'S WORKPLACE AND SPECIFYING THE ACTIONS THAT WILL BE TAKEN AGAINST EMPLOYEES FOR VIOLATIONS OF SUCH PROHIBITION; (III) STATE IN ALL SOLICITATIONS OR ADVERTISEMENTS FOR EMPLOYEES PLACED BY OR ON BEHALF OF THE CONTRACTOR THAT THE CONTRACTOR MAINTAINS A DRUG-FREE WORKPLACE; AND (IV) INCLUDE THE PROVISIONS OF THE FOREGOING SECTIONS I, II, AND III IN EVERY SUBCONTRACT OR PURCHASE ORDER OF OVER $10,000, SO THAT THE PROVISIONS WILL BE BINDING UPON EACH SUBCONTRACTOR OR CONTRACTOR.

FOR THE PURPOSE OF THIS SECTION, "DRUG-FREE WORKPLACE" MEANS A SITE FOR THE PERFORMANCE OR WORK DONE IN CONNECTION WITH A SPECIFIC CONTRACT AWARDED TO A CONTRACTOR IN ACCORDANCE WITH THIS CHAPTER, THE EMPLOYEES OF WHOM ARE PROHIBITED FROM ENGAGING IN THE UNLAWFUL MANUFACTURE, SALE, DISTRIBUTION, DISPENSATION, POSSESSION OR USE OF ANY CONTROLLED SUBSTANCE OR MARIJUANA DURING THE PERFORMANCE OF THE CONTRACT.

NONDISCRIMINATION CLAUSE:
1. EMPLOYMENT DISCRIMINATION BY OFFEROR SHALL BE PROHIBITED.
2. DURING THE PERFORMANCE OF THIS CONTRACT, THE SUCCESSFUL OFFEROR SHALL AGREE AS FOLLOWS:

   A. THE OFFEROR, WILL NOT DISCRIMINATE AGAINST ANY EMPLOYEE OR APPLICANT FOR EMPLOYMENT BECAUSE OF RACE, RELIGION, COLOR, SEX, NATIONAL ORIGIN, AGE, DISABILITY, OR ANY OTHER BASIS PROHIBITED BY STATE LAW RELATING TO DISCRIMINATION IN EMPLOYMENT, EXCEPT WHERE THERE IS A BONA FIDE OCCUPATIONAL QUALIFICATION/CONSIDERATION REASONABLY NECESSARY TO THE NORMAL OPERATION OF THE OFFEROR. THE OFFEROR AGREES TO POST IN CONSPICUOUS PLACES, AVAILABLE TO EMPLOYEES AND APPLICANTS FOR EMPLOYMENT, NOTICES SETTING FORTH THE PROVISIONS OF THIS NONDISCRIMINATION CLAUSE.

   B. THE OFFEROR, IN ALL SOLICITATIONS OR ADVERTISEMENTS FOR EMPLOYEES PLACED ON BEHALF OF THE OFFEROR, WILL STATE THAT SUCH OFFEROR IS AN EQUAL OPPORTUNITY EMPLOYER.

   C. NOTICES, ADVERTISEMENTS, AND SOLICITATIONS PLACED IN ACCORDANCE WITH FEDERAL LAW, RULE OR REGULATION SHALL BE DEEMED SUFFICIENT FOR THE PURPOSE OF MEETING THE REQUIREMENTS OF THIS SECTION.

   D. OFFEROR WILL INCLUDE THE PROVISIONS OF THE FOREGOING SECTIONS A, B, AND C IN EVERY SUBCONTRACT OR PURCHASE ORDER OF OVER $10,000, SO THAT THE PROVISIONS WILL BE BINDING UPON EACH SUBCONTRACTOR OR CONTRACTOR.

Name and Address of Offeror:

_____

_____

_____

E-mail Address:_____
Telephone Number:__(____)_____
Fax Phone Number: _(____)_____
FIN/SSN #:_____

Date: _____

By: _____
Signature in Ink

_____
Printed Name

_____
Title

Is your firm a "minority" business? □ Yes □ No If yes, please indicate the "minority" classification bellow:
□ African American □ Hispanic American □ American Indian □ Eskimo □ Asian American □ Aleut
□ Other; Please Explain: _____
Is your firm Woman Owned? □ Yes □ No
Is your firm a Small Business? □ Yes □ No
Is your firm Service Disabled Veteran Owned? □ Yes □ No

City of Virginia Beach – Purchasing Division
Subcontracting Participation Plan
For Goods and Services

Form CVAB – GS1

Project Name: _____

Bid/RFP Number: _____

Vendor: _____

Address: _____

City, State, Zip: _____

Contact Telephone: _____

Contact Email: _____

Project Name: _____

Total Bid/RFP Amount

Total Subcontracting Amount

Intent to utilize subcontractors ☐**Yes** ☐**No** (If Vendor intends to self-perform all work, check "NO" and skip to Signature Line below)

Firm/individual Name	Number (If certified with SBSD*)	Status (M, S, or W)	Scope of work to be Performed	Estimated Subcontractor Dollar Amount (if Known)	SBSD* Certified Y/N	MBCoord Approval (FOR OFFICE USE ONLY)	Verified

IMPORTANT: PLEASE SUBMIT THIS PARTICIPATION PLAN WITH YOUR BID/RFP

By signing below, you attest that the above information is true and accurate to the best of your knowledge.

Authorized Representative(Prime) Print Name	***Title***	***Authorized Representative (Prime) Signature***	***Date***

SBSD = Virginia Department of Small Business and Supplier Diversity

Table of Contents

Table of Contents

List of Tables

I. PURPOSE

The City of Virginia Beach (City) intends to procure a secure, diverse, and redundant public safety communication network based on Internet Protocol ("IP") technologies. The purpose of this request for proposals is to solicit solutions to empower the City of Virginia Beach to adopt solutions that will allow the City's emergency services providers and dispatchers to more effectively deal with the rapidly evolving IP based communication services, both fixed and mobile, used by the citizen and visitors to the Virginia Beach area. The selected solution will allow the City of Virginia Beach to make forward looking and economically sound decisions regarding the upgrade of public safety and first responder mission critical infrastructure.

II. BACKGROUND

The City of Virginia Beach ("City") is preparing for a migration from legacy, circuit-switched 9-1-1 with limited interoperability to a Next Generation 9-1-1 ("NG9-1-1") regional system built on a standards-based Emergency Services IP [Internet Protocol] Network ("ESInet") that will enable seamless interoperability across the region. This Request for Proposal ("RFP") is the first step in progressing toward the City's vision of regional interoperability.

The City has the option to join the ESInet solution proposed for the National Capital Region ("NCR"); however, the City is interested in soliciting bids from all interested NG9-1-1 solutions providers to ensure the citizens of the City have the best emergency number system currently available. The State of Virginia Information Technologies Agency ("VITA") is actively encouraging, promoting, and assisting local jurisdictions in migrating to NG9-1-1 systems. VITA's grant funding activities for NG9-1-1 deployment require that ESInets deployed in the Commonwealth of Virginia be capable of interoperability with other ESInets. The City expects the Offeror to clearly address operations in a multi-ESInet environment that will provide interoperability throughout the Commonwealth as well as neighboring states. Also, the City is looking for Offerors to address the integration of independent neighboring communities to City into a regional ESInet.

The City's existing emergency communications infrastructure consists of a single consolidated call handling and dispatch center. Currently, there is no hot standby location. There are plans to establish a backup center, but as of the time of this RFP there is no clearly defined location. Offerors should detail the interoperability of their solution with other ESInets from different providers to allow the City the option of directing emergency calls to a suitably equipped destination outside the City.

Other jurisdictions within the Tidewater region and throughout the Commonwealth of Virginia may wish to participate in the resulting award with the City. Each jurisdiction will procure its service through this RFP and contract with the contractor independently. That stated, the primary goal of this RFP is for the procurement of NG9-1-1 services for the City.

The City desires that Next Generation Core Services ("NGCS") vendors provide the call routing intelligence required by a next generation system. The functional elements include transitional elements as well as NGCS, including, but not limited to, the following:

- Legacy Network Gateway - LNG
- Legacy PSAP Gateway - LPG
- Border Control Functions - BCF
- Emergency Services Routing Proxy - ESRP
- Policy Routing Function - PRF
- Emergency Call Routing Function - ECRF
- Location Validation Function - LVF
- Location Database - LDB
- Spatial Interface - SI

- PSAP Interfaces
- Discrepancy Reporting
- Event Logging
- Time Server

III. SCOPE OF WORK

A. GENERAL REQUIREMENTS

1. Project Knowledge

a) Responses to Each Requirement

The responses to each requirement described in this RFP must include one of the following:

- **Understood:** The Offeror understands the statement without question or providing clarification.
- **Complies:** The Offeror proposal complies with the RFP requirements and the products/services are included in the base price, are currently developed, and are available for implementation (i.e., must be generally available).
- **Complies Partially:** The Offeror proposal addresses the RFP requirements through another method that is currently developed and is available for implementation (i.e., must be generally available) or the solution complies with some, but not all, of the requirements. Offeror is responsible for clearly explaining how its proposed solution does not fully comply.
- **Complies with Future Capability:** The RFP requirements will be met with a capability delivered at a future date. This response must include a calendar quarter and year that the requirement will be met with a generally available product or service at no additional cost.
- **Does Not Comply:** The Offeror proposal does not/cannot meet the specific RFP requirement.

1. Below each requirement will be either one (Understood) checkbox or four checkboxes (Complies, Complies Partially, Complies with Future Capability, Does Not Comply). Offeror must respond by placing an "X" in only **one** checkbox per stated requirement. Failure to complete this process properly will be treated the same as "Did Not Answer."

   ☐ Understood

2. A response and description to each requirement is required. Do not underestimate the importance of providing details. The details should be sufficient to properly convey Offeror's intentions, but should not be verbose in nature. Marketing materials are not considered appropriate in-line responses. Offeror may attach marketing materials as separate, supplemental documents, but details are still required to support the answer.

   ☐ Understood

3. Offeror shall not refer to other sections as a response. Even if the response is an exact duplicate of a previous response, the details must be provided in the same paragraph as the requirement. Offeror must not include pricing information in its description and must not refer the reader to pricing; note that the City's evaluation team(s) members will not have access to pricing information.

   ☐ Understood

2. Offeror Vision of NG9-1-1

The City is interested in retaining the Offeror most clearly demonstrates its alignment with the industry's evolution to National Emergency Number Association ("NENA") NGCS solutions. Each Offeror shall describe its vision of NG9-1-1 and how it aligns with NENA's vision.

Also noteworthy would be items such as position papers or partnerships/alliances intended to further the vision of the NGCS. All proprietary documents must be clearly marked.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

3. Single Point of Contact

The successful Offeror shall be the contractor of record and serve as the City's single point of contact (Prime) for proposals and any contract that may result from this RFP. The Prime is responsible for any partners or subcontractors.

☐ Understood

4. Information Provided By the Offeror

Offeror is solely responsible for conducting its own independent research, due diligence, or other work necessary for the preparation of responses, negotiation of contracts, and the subsequent delivery of services pursuant to any contract resulting from this RFP. The City takes no responsibility for the completeness or the accuracy of any information presented in this RFP or otherwise distributed or made available during this selection process or during the term of any subsequent contract.

☐ Understood

B. TECHNICAL REQUIREMENTS

1. Capacity

1. All IP network components, physical network segments, and NGCS elements shall support each PSAP's current call handling capacity, plus 25-percent growth over the life of the initial contract. All networks and NGCS elements shall be designed with no single points of failure. All equipment shall be new and of current manufacture. Used, refurbished, or end-of-life equipment shall not be used.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

2. If the Offeror's solution is rate limited, Offeror shall state the maximum number of calls per second that the proposed solution can sustain. Offeror also should specifically address how multimedia and text calls will affect call handling capacity.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

2. Standards

The City seeks a standards-based solution that complies with all applicable NENA, Association of Public-Safety Communications Officials ("APCO"), American National Standards Institute ("ANSI"), and Internet Engineering Task Force ("IETF") standards. Proprietary solutions or solutions with limited compliance with industry standards may be disqualified if it is determined the solution will not immediately achieve the City's goal of interoperability throughout the region with neighboring legacy Selective Routers ("SRs") and with future neighboring ESInets.

As industry standards evolve, the contractor's solution shall continue to comply with industry standards. Specifically, the contractor's solution shall comply with new NGCS and ESInet industry standards within 18 months of ratification of applicable industry standards. This applies to current and future revisions of the following list of standards and the supporting standards referenced within each standard. As solution updates are made to maintain industry standards compliance, the solution shall not abandon services or feature functionality in place at the time of the solution upgrade. Applicable industry NG9-1-1 standards and informational documents include, but are not limited to:

- NENA-STA-010.2-2016, Detailed Functional and Interface Specification for the NENA i3 Solution, and its successors.
- NENA 75-001, Security for Next Generation 9-1-1 Standard ("NG-SEC") and its successors
- NENA-INF-016.7-2018 Emergency Services IP Network Design for NG9-1-1 Information Document, Version 1, and its successors
- NENA-STA-003.1.1-2014, NENA Standard for NG9-1-1 Policy Routing Rules and its successors
- NENA-REQ-002.1-2016, NENA Next Generation 9-1-1 Data Management Requirements and its successors
- NENA-STA-004.1.1-2014, NENA Next Generation 9-1-1 United States Civic Location Data Exchange Format ("CLDXF") and its successors
- NENA-INF-027.1-2018, NENA Information Document for Location ValidationFunction Consistency
- APCO NENA 2.105.1-2017, NENA/APCO Emergency Incident Data Document ("EIDD"), to be replaced by its eventual ANSI document
- NENA-STA-006.1-201x, NENA GIS Data Model for NG9-1-1
- IETF Base IP Protocols
- IETF IP Routing Protocols such as Border Gateway Protocol ("BGP") and Open Shortest Path First ("OSPF")
- IETF Session and Media Protocols such as Session Initiation Protocol ("SIP"), Session Description Protocol ("SDP"), Message Session Relay Protocol ("MSRP"), and Real-Time Transport Protocol ("RTP")
- IETF Protocols such as Location-to-Service Translation ("LoST"), HTTP-Enabled Location Delivery ("HELD"), and Presence Information Data Format Location Object ("PIDF-LO")

Offeror shall reveal any use of proprietary standards or protocols in its proposed solution or state that it fully complies with this requirement. Any limitations, whether technological or philosophical, shall be disclosed in the response.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

The City's has included its information technology standards in Attachment B – City of Virginia Beach Computing Environment and Information Technology Standards. It is expected that Offerors comply with all applicable provisions of Attachment B, most notably Section R – Hosted Solutions.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

3. Network

1. Offeror must include in its proposal the fully functional ESInet services capable of supporting the City's primary location and any future backup center located in the region. Also, Offeror must provide backup and secondary interconnectivity with AT&T/West, an ESInet provider to other regions in the Commonwealth of Virginia as well as the District of Columbia Office of Unified Communications. Contractor will have to interconnect with other regional and State-level ESInets in the future, at which time scope and costs will be assessed.

   ☐ Understood

2. As defined in NENA-STA-010.2-2016, "An ESInet is a managed IP network that is used for emergency services communications, and which can be shared by all Public Safety agencies. It provides the IP transport infrastructure upon which independent application platforms and core functional processes can be deployed, including but not limited to, those necessary for providing NG9-1-1 services. ESInets may be constructed from a mix of dedicated and shared facilities. ESInets may be interconnected at local, regional, state, federal, national and international levels to form an IP-based internetwork (network of networks).

   The City's desire is to implement a redundant, resilient, public safety grade (99.999 percent uptime), managed, IP-based ESInet. This shall be a managed router solution ESInet. Contractor shall design such a network to provide the infrastructure for NENA i3 core services and processes ("NGCS") while interconnecting and providing interoperability for the City's primary PSAP location and the City's Back Up Site, as well as other locations shown in Attachment C - City of Virginia Beach PSAPs And List of Preferred Interoperable Agencies.

   ☐ Understood

3. The network shall be designed with, at a minimum a dual core network design with geographically diverse network-to-network interfaces ("NNIs"). For this RFP, a **network-to-network interface** (NNI) is an interface that specifies signaling and management functions between two carrier networks. An NNI circuit can be used for interconnection of signalling (e.g., SS7), Internet Protocol (IP) (e.g., MPLS) or ATM networks.A minimum of one NNI shall be located within the Local Access Transport Area ("LATA") of the City of Virginia Beach. The design shall use, where available, diverse entrances (e.g., "east-west" entrance(s) into each facility that is a part of the City's ESInet, including data centers, PSAPs, and other locations. The primary and redundant links shall be engineered to not share common NNIs, transport routes, trenches, or poles. If facility construction is required, Offeror shall so indicate. In the event that diverse entrances or diverse right of ways are not possible at a given location, Offeror shall indicate how it intends to provide redundant and resilient connectivity to that location. The City is open to proposals that provide nonterrestrial

transport if priced as an option. The ESInet shall be capable of IP interconnection to the Public Switched Telephone Network ("PSTN") for outbound local and long-distance calling.

☐ Understood

4. All network equipment shall be new and of latest version manufacture and include current manufacturer support date estimates. All servers, systems, routers, switches, and other network equipment shall support IPv4 and IPv6 and be capable of running dual protocol stacks.

   ☐ Understood

5. The City's view of the network shall be at Layer 3 of the International Organization for Standardization ("ISO") model (i.e., IP packets are routable between any two points on the ESInet). The network shall comply with Institute of Electrical and Electronics Engineers ("IEEE") 802.3 Ethernet standards, as well as the IETF Requests for Comments ("RFCs").

   ☐ Understood

6. Internal ESInet network routing shall be accomplished through use of the Open Shortest Path First ("OSPF") protocol, as defined in RFC 2328 and RFC 5340 External network routing, such as that to service providers and other ESInets, shall be through the use of the Border Gateway Protocol ("BGP") as defined in IETF RFC 4271. All routing protocols shall implement authentication between neighboring routers. Other standards-based protocols may be considered by the City, but the use of proprietary routing protocols is prohibited.

   ☐ Understood

7. Resiliency, or fast failover, may be achieved through the use of the Bidirectional Forwarding Detection ("BFD") protocol as defined in IETF RFC 5880 and RFC 5881 or other standards-based, non-proprietary methods approved by the City.

   ☐ Understood

8. All routers and switches must support multicast routing and switching. The applicable base protocols are Internet Group Management Protocol ("IGMP") and Protocol Independent Multicast ("PIM"). These protocols handle the routing of join and leave requests for the multicast streams across both local and wide area networks. IGMP version 3 ("IGMPv3") is the most current version and is defined in RFC 3376. This RFC was amended by RFC 4604, which added Multicast Listener Discovery ("MLDv2"), which provides the equivalent functionality for IPv6. There are four varieties of PIM: sparse mode ("RFC 4601"), dense mode ("RFC 3973"), bidirectional mode ("RFC 5015"), and source-specific mode ("RFC 3569").

   ☐ Understood

9. The network equipment shall support Quality of Service ("QoS") marking for prioritizing traffic in the network using the Differentiated Services Code Point ("DSCP") protocol. While the network can change DSCP values through rules, the values typically are set by the system or functional element that originates the traffic. Network routers and switches shall not be configured in such a manner as to change DSCP values set by originating functional elements.

   ☐ Understood

10. The proposed ESInet shall be private, robust, scalable, secure, diverse, redundant, and sustainable. Offeror shall identify any single point of failure paths or equipment included in their

proposal. Offeror shall propose a network solution for all List of Preferred Interoperable Agencies sites listed in Attachment C. It is understood that while the future sites are outside the scope of this initial offering, however, Offerors should address future interoperability requirements.

☐ Understood

11. Contractor is responsible for any third party certification fees.

☐ Understood

12. Offeror shall describe how its proposed solution meets each of the requirements outlined in Section 4.3.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

13. Using the information provided in Attachment C Section I, the City's primary location and backup locations, Offeror shall provide the proposed bandwidth for each PSAP. The bandwidth calculations for PSAPs served by hosted call handling systems should be included in the host site's bandwidth. If the PSAP's current trunking, position count, and call volume places its proposed bandwidth within 80 percent of being fully utilized, then Offeror shall provide an indication of the next higher tier of bandwidth and include a corresponding line item in the optional pricing table.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer.

4. Interconnection to Legacy Selective Routers

1. Contractor must provide a network design that will allow legacy PSAPs to transfer calls to the City ESInet. See Attachment C, Section III for a list of all Preferred Interoperable Agencies that will require interconnection to the Legacy Selective Router to maintain current 9-1-1 service levels. This design shall also include a method for the City to obtain location information on the transferred call. This legacy compatibility shall be redundant and resilient. It may include LNGs, but the design should be capable of Legacy Selective Router Gateway ("LSRG") functionality to allow the legacy SRs to transfer calls with Automatic Number Identification ("ANI") and obtain Automatic Location Identification ("ALI") information for the City's NGCS and vice versa. LSRG functionality shall allow for legacy PSAPs served by legacy SRs to serve as the abandonment route for City PSAPs served by the contractor's ESInet and NGCS.

   The design should allow for the storage and update and dialing of special selective router directory numbers ("DNs") to effect transfers from ESInet PSAPs to legacy PSAPs still operating on the selective routers. Conversely, the LSRG shall be able to convert calls transferred to ESInet PSAPs with DNs to the appropriate uniform resource identifier ("URI") for delivery of the call to the NG9-1-1 PSAP.

   ☐ Complies

☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

2. Offeror shall explain how it has worked with legacy selective router providers with similar solutions on similar projects and shall provide specific plans for working with the City's legacy 9-1-1 service provider, Verizon.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

3. Offeror shall explain how incidents of existing Rate Centers being split between the legacy 9-1-1 system and the City of Viriginia Beac ESInet or other provider ESInets shall be deployed and managed after the City of Virginia Beach migrates to the ESInet. The details should include enumeration of Offeror's expectations of communication service providers to provide subscriber information for emergency calls.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

5. Interconnection to Other ESInets

The City's jurisdiction is served by a single call center. However, the ability to interconnect for the exchange of emergency calls to jurisdictions surrounding the City, as well as other areas of the Commonwealth of Virginia and the State of North Carolina is crucial to effect emergency response in the Tidewater region. In addition, Washington, DC, and jurisdictions in the NCR of northern Virginia have, or are in the process of deploying, NG9-1-1 call routing services from AT&T/West. Specifically, both jurisdictions have independently deployed, or are in the process of deploying, IP-based emergency call routing services, and it is anticipated there eventually will be a migration to geospatial routing using NENA i3 protocols during the initial term of the City's NGCS services. Similar to the need for legacy SRs to interoperate, the City requires interoperability on Day 1 between neighboring ESInets that may provide IP-based Selective Routing ("IPSR") services or NGCS to their PSAPs. See Attachment C, Section IV for a list of all Preferred Interoperable Agencies that may require ESInet to ESInet interconnection.

Offeror shall describe how its proposed solution will seamlessly interwork with AT&T/West and other neighboring ESInets that serve their clients with IPSR and/or NGCS. Offerors shall assume that interconnection with other ESInet providers may require multiprotocol label switching ("MPLS") handoff at an ESInet provider designated locations which may be outside of Virginia. Offerors shall provide a specific plan, including costs, for interoperating with Washington, DC, and other ESInet systems being deployed in the northern Virginia area. This should include all One Time Fees in the Cost Proposal. The

design should specify whether interconnection will be at the data center or the carrier NNI level, and all necessary transport links for conveyance of traffic over the design shall be diverse and redundant.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

6. Interoperability with State Police, Military Bases, and Other Federal Entities, Colleges and Universities

1. The City contains several military bases and other Federal institutions that have special security and first responder operations. In many cases, the Federal entity has Centralized Automated Message Accounting ("CAMA") trunks from the legacy SRs and is able to bid ALI, providing for the ability to receive call transfers with ANI and ALI information. Meanwhile, State police PSAPs send and receive all transfers via 10-digit lines without ANI and ALI information.

   Offeror shall describe how it can provide the same or improved capability for these special secondary PSAPs. Optional pricing is requested for potential future addition of these entities. Offerors shall assume these sites have legacy customer premise equipment ("CPE"), fewer than 10 CAMA trunks, and fewer than 10 positions.

   - ☐ Complies
   - ☐ Complies Partially
   - ☐ Complies with Future Capability
   - ☐ Does Not Comply

   Details to support the answer:

7. Data Centers

The network and NGCS are provided by an array of firewalls, routers, gateways, and servers. The servers may include Storage Area Network ("SAN") or Network Attached Storage ("NAS") devices, which are high-capacity, redundant (i.e. the data should be replicated to the vendor's cloud as part of the disaster recovery component), resilient hard disk storage systems. These are the types of devices that will be housed in multiple geo-diverse data centers. If the decision is made to co-locate a hosted call handling system in these centers, those systems also will be comprised of similar equipment. These devices typically are mounted in four-post lockable cabinets rather than open racks.

Offeror shall provide descriptions of previous data center implementations for similar solutions, along with specific details for the Offeror-recommended solution.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

a) Data Center Locations

1. The City requires a minimum of two geo-diverse data centers to house the NGCS. The host data centers must provide sufficient geo-diversity to provide physical diversity in case of a widespread

disaster. Optimally, the City desires that at least one of the proposed data centers be within a 50-mile radius of the City footprint, but it is not required. The proposed solution should include at least two data center locations for hosting NGCS. Additional data centers may be required for hosting LNGs serving the region. A value proposition for implementing or not implementing a third data center, which could be taken offline for testing software, is desirable. Each data center shall be able to support 100 percent of the expected 9-1-1 communications in a failover mode.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

2. The Offeror shall provide examples of its implementation of NGCS in multiple data centers similar to the proposed solutions. Details, including sample drawings, shall be provided supporting the proposed data center solution.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

b) Data Center Requirements

The data centers should meet, at a minimum, Tier 3 design standards as detailed in Telecommunications Industry Association ("TIA") 942, Data Center Standards. Design standards include, but are not limited to, the following:

- Redundant commercial power (supplied from separate grids if possible)
- Redundant backup generators
- Redundant uninterruptible power supplies ("UPS")
- Redundant heating, ventilation, and air conditioning ("HVAC") systems
- Fire suppression systems
- Physical access security
- Physically separate communication service provider entry points
- Data Centers utilized will be located within the continental United States

ANSI/TIA-606-B governs the operation and administration of data centers. It covers such topics as space and equipment labeling, cable labeling and color coding, cable classes, and grounding and bonding. This standard lays out a complete marking standard for data centers using a 2-foot grid of the room and designating each square with letters and numbers starting at AA01. All cabinets, racks, patch panels, and devices within said cabinets and racks should be identified and labeled front and rear.

All City systems and network equipment shall be housed either in a locked and monitored cage within a secure data center or in its own locked and monitored room within a secure data center. Simply providing space in a common area is not acceptable. Offeror shall provide a description and cost for the City to authorize personnel for access to data center cages.

The Offeror shall provide detail regarding how its proposed solution meets these requirements. These details will include specifics regarding certifications that confirm these requirements are met.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

c) Cabinets and Power Distribution

1. Cabinets shall be fully enclosed and lockable. The front and rear doors may be vented or solid. If the doors are solid, adequate ventilation must be provided to remove the heat from the cabinet.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

2. Many options are available for power distribution units ("PDUs") that provide power inside the cabinets. At a minimum, the PDU should be remotely manageable via the Simple Network Management Protocol ("SNMP") and provide load information back to the network management system. Given the wide geographic dispersion of the data centers, it is advisable to consider PDUs that have individually controllable outlets in order to remotely power-cycle equipment that otherwise may be unresponsive. This ability should be coupled with remotely accessible console servers to allow console access into devices in the data centers.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

d) Support Maintenance

1. Offeror shall describe in detail its 24 hours a day, 7 days a week, 365 days a year (24/7/365) maintenance support for the life of the service-based solution. Offeror shall describe its understanding of public safety maintenance windows and associated notification processes. Offeror shall describe its problem and change management processes and supporting systems and its adherence to best practices, such as those described in Information Technology Infrastructure Library ("ITIL") version 3.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

8. Security

1. The security requirements apply equally to all elements of the system requested in this RFP, including, but not limited to, the following:

- Data centers
- PSAPs
- ESInets
- NGCS elements
- Other facilities housing any element or device that is a part of the overall system

The proposed solution's security program is required to use the latest NENA specifications and incorporate the intentions of the Communications Security, Reliability and Interoperability Council ("CSRIC") "Best Practices."[1] All applicable rules and regulations of the Federal Communications Commission ("FCC"), in addition to those specified herein, shall apply.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

2. Offeror shall provide a compliance matrix, as outlined in NENA 75-502, NENA Next Generation 9-1-1 Standard ("NG-SEC") Audit Checklist, which identifies whether it's proposed solution Complies (C), Does Not Comply (No), or is Not Applicable (N/A) to the identified requirement(s) for each audit question, using the instructions provided in Section 3 of NENA 75-502. If N/A is provided, Offeror shall provide an explanation as to why the question is not applicable to the proposed solution.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

3. Offeror shall describe its capabilities to provide predictive analysis and modeling to combat security threats.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

4. The Offeror's proposed solution shall provide a process so that devices and carriers outside the ESInet shall not have credentials, per NENA-08-003 or its successor document. The Offeror shall provide details regarding how its proposed solution ensures that devices and carriers outside the ESInet are not provided credentials.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

[1] As found at http://transition.fcc.gov/pshs/advisory/csric; WG1A, WG2A, WG2B, WG4A, WG4B, WG4C, WG5A, WG6, WG7 and WG8.

Details to support the answer:

5. Contractor shall allow for annual third party security audits at the request and cost of the City.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

6. A comprehensive security plan is a critical component of the City's NGCS solution. The Offeror shall describe its security plan, monitoring processes, and incident response processes, including procedures related to communication with the City should a breach or other incident occur.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

a) Physical Security

1. All facilities' housing components of the City ESInet and NGCS shall have security and access control systems that ensure only duly authorized individuals can access the areas housing the City's systems and network equipment. Any workstations or other PSAP equipment connected to the ESInet shall be housed in secured, access-controlled areas. Any devices, power distribution, and cross-connect panels feeding the cages or rooms housing the City's systems shall be similarly protected. The offerer will also provide a recent SOC II report for each data center utilized in the proposal.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

2. Contractor, upon request, shall furnish monthly reports on physical access to the City ESInet and NGCS facilities, including failed attempts.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

9. Network Operations Center/Security Operations Center

1. All components of the proposed solution shall be monitored 24/7/365 by a centralized Network Operations Center ("NOC") and Security Operations Center ("SOC"). These functions may be in separate facilities or combined in a single facility.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

2. Offeror shall describe its NOC/SOC operations model, continuity of operations ("COOP") plan, problem and change management systems, reporting systems, escalation plan, and conformance with best practices for service delivery management.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

a) Security Monitoring and Management

1. The contractor's security management solution shall control access to network resources according to public safety network security guidelines to prevent sabotage (intentional or unintentional) and the compromise of sensitive information. Security management shall use public safety network security standards to monitor users logging into network resources and refuse access to those who enter inappropriate access codes. The proposed IP-enabled network shall support standard security policies that may include the use of firewall rules, access control lists ("ACLs"), virtual local area networks ("VLANs"), virtual private networks ("VPNs"), and Secure Sockets Layer ("SSL") protocols to control network traffic and access. The systems and servers shall support the use of software to detect and mitigate viruses, malware, and other attack vectors.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

2. Furthermore, any system that connects to an IP-enabled network shall be required to comply with applicable standards, including security standards, and demonstrate compliance through an initial and recurring audit.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

3. Contractor shall provide security reports on a monthly basis, including, but not limited to, incidents and incident response and updates or changes to security systems and software.

☐ Complies
☐ Complies Partially

☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

4. Offeror shall provide details concerning how its proposed solution will provide for security monitoring and management. Offeror shall provide details, including drawings that explain how its proposed solution meets or exceeds the above requirements.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

b) Incident Management System

The contractor's incident management system shall log all support requests, both from users and those automatically generated. The Offeror shall provide examples of monthly reports detailing tickets opened, resolved, and pending.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

c) Change Management System

1. The change management system shall log all change requests, both from users and those automatically generated. The system shall interface with the incident management system for correlation of changes and outages. The Offeror shall describe its change management process and its ability to provide the City Program Manager with the ability to review proposed change requests and the client approval process. The contractor shall provide monthly reports detailing change tickets opened, resolved, and pending.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

2. The Offeror shall provide detailed descriptions of any other tools it intends to use in order to provide access to the change management system, such as Web portals and client software.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

d) Management Software

1. Much is said about SNMP in network and server management discussions, but it is only the underlying protocol for transporting management information across the network. Software packages are widely available for capturing, analyzing, and reporting the network's health based on the SNMP traffic it receives. Several commercial packages are available, such as SolarWinds, Monolith, and OpenView, as well as many full-featured open source packages, such as OpenNMS, Nagios, and Network Management Information System ("NMIS").

   Offeror shall provide the name and description of the management software it has implemented, including all functional modules associated with it (e.g., reporting, backup, IP address management).

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

2. Offeror shall provide a detailed explanation and associated drawings explaining how its proposed solution interworks with all of the various elements and services of the total City NG9-1-1 solution and meets or exceeds the above requirements.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

e) Network and System Event Logging

1. The IP network and the NGCS shall allow historical tracking of network and system events, as well as event resolution. This is for logging errors and statistical information related to the health of the network and the NGCS.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

2. It is preferable this system be part of, or interfaced with, the various contractor and supplier trouble ticketing systems, or contain cross-reference abilities. Contractor shall maintain historical information for the term of the contract and provide copies of the data to the City at the end of the contract.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

Details to support the answer:

3. Offeror shall provide a detailed explanation and associated drawings explaining its processes and procedures for interfacing with the Offeror and supplier solutions. Offeror shall provide details regarding how its proposed solution meets or exceeds the above requirements.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

f) Physical Access Monitoring and Management

1. Contractor shall track and log all attempts to access the cabinets, data center cage, or rooms housing the NGCS components serving the City. Reports may be requested and shall be made available for review as part of problem management reporting.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

2. Offeror shall provide a detailed explanation of its processes and procedures for logging physical access to the NGCS components and how it generates the required reports.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

g) Access to Technical Staff

The contractor shall detail the procedures by which it communicates with technical personnel from participating suppliers and the City entities. The Offeror shall specify the level of assistance expected from such technical personnel to resolve service-related issues. Security personnel are expected to recommend solutions to various malicious network activities. Offeror shall provide a detailed explanation and associated graphical presentations explaining how its proposed solution meets or exceeds the above requirements.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

h) Notification

Offeror shall specify how its NOC informs participating jurisdictions or their designee of problems with the network, scheduled outages, and upgrades. Tickets related to the services delivered to contractor suppliers shall be forwarded automatically. Notification shall be provided via multiple communications means to City entities. Entities requiring notification may change, depending on the alarm or incident. Offeror shall provide a detailed explanation explaining how its proposed solution meets or exceeds the above requirements. Offeror, as a NG9-1-1 services provider, shall also describe their understanding of the reporting requirements for 9-1-1 services at both a State and national level.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

i) Escalation Procedures

Offeror shall outline a detailed jurisdiction-level escalation process to be used during incidents that affect service, particularly those that result in critical service outages. Offeror shall describe how discrepancies in the perception of service level agreement ("SLA") incident levels may be escalated and addressed. It is preferable that these procedures be maintained and accessible via an online portal. This notification shall be integrated with the notification processes described above based on alarm or incident. Offeror shall provide a detailed explanation explaining how its proposed solution meets or exceeds the above requirements.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

j) Change Management Processes and Procedures

Offeror shall outline a detailed change management process. The ITIL change management practices are preferred, but not required. Offeror shall include explanation of its fault, configuration, accounting, performance, and security ("FCAPS") procedures. Offeror shall provide a detailed explanation explaining how its proposed solution meets or exceeds the requirements for the ITIL and FCAPS processes.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

k) Statement on Standards for Attestation Engagement Number 16

Contractor shall demonstrate compliance with the Statement on Standards for Attestation Engagements Number 16 ("SSAE 16"). This replaced the Statement on Accounting Standards 70 ("SAS 70") in 2011. The applicable report from an SSAE 16 engagement is the Service Organization Controls 1 ("SOC 1") report.

Offeror shall provide a detailed explanation of how it has complied with SSAE 16 for similar solutions and how this would be implemented with the City NG9-1-1 implementation. The Offeror shall provide with its detailed explanation a graphical representation explaining how its proposed solution meets or exceeds the above requirement.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

l) Configuration Backup and Restoration

The contractor and various suppliers shall deploy the capability to automatically or routinely back up configuration data and define the conditions under which it will restore the configuration of network elements, such as routers or switches, and the process it will use should the need arise.

In addition to automatic, regular backups, contractor and the various suppliers shall describe their ability to perform on-demand backups, such as at the end of a successful configuration change.

The Offeror shall provide a detailed explanation and any associated drawings explaining how its proposed processes and procedures provide the ability to manage these configuration backup and restoration processes in a manner that has no negative impact on the total City NG9-1-1 solution.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

m) Third Party Management

The City desires the optimum value provided by best-of-class products and services integrated as part of its total NG9-1-1 solution. This may present a situation where no single manufacturer or supplier can provide a public safety-grade unified NOC/SOC accountability for all components, products, and services that comprise the City's total NG9-1-1 solution. Consequently, the City may find it beneficial to have a third party provide that overarching NOC/SOC service.

A third-party NOC/SOC provider may be responsible for functioning as an umbrella for monitoring all of the contractor's products and services, including collaboration with the contractor's NOC/SOC. To facilitate that capability, the third party NOC/SOC must have a view into all elements that are under SLAs.

In support of the City's consideration of such an option, Offeror shall indicate the compliance level of its experience in providing access to third party NOC/SOC overarching support, as related to the requirements identified in the following table (**Table 1**).

Table 1. Third Party NOC/SOC Support

Requirement	Complies	Complies Partially	Complies with Future Capabilities	Does Not Comply
4.9.13.1 Change management processes				

Requirement	Complies	Complies Partially	Complies with Future Capabilities	Does Not Comply
4.9.13.2 Coordinating and managing trouble tickets to resolution from contractor and multiple suppliers				
4.9.13.3 Trouble ticket report management (reports may be daily, weekly, monthly, quarterly, or yearly)				
4.9.13.4 Notification processes for contractor and suppliers and any other entities or people designated by the City				
4.9.13.5 System alarm access in the form of SNMP or syslog data				
4.9.13.6 Experience and processes for interworking of multiple public safety voice and data system suppliers				

n) Operational Scenarios

The City recognizes that no system or staff is perfect; however, safeguards may be established to minimize the impact of human or system error. Offeror shall describe its risk mitigation and issue resolution strategies for the following hypothetical scenarios:

1. At 0300 hours, a series of session border controller alarms previously unseen by the NOC staff on duty begin to increase in volume and frequency. At 0330, multiple critical alarms are received, and the City call center reports they have not received a call in the last 15 minutes nor can they dial outbound on ESInet PSTN lines. At 0345, a few PSAPs start reporting garbled audio, while others report an inability to obtain location information.

   Response to hypothetical scenario:

2. All originating service providers with subscribers in the City are directly connected via Signaling System 7 ("SS7") to the Offeror's two LNGs that are dedicated to the City for ingress emergency calls. Each LNG consistently processes about 10,000 calls per day, but each is capable of processing in excess of 100,000 calls per day. On Monday at 12:17 a.m., one of the LNGs experiences a catastrophic failure and is unable to process any calls. In a review of Monday's logs, it is found that the surviving LNG processed only 14,000 calls.

   Response to hypothetical scenario:

3. As part of normal data maintenance procedures, the City jurisdiction has uploaded six minor recent changes to its road centerline data. The Offeror's SI quality assurance/quality control ("QA/QC") process provides a discrepancy report detailing 15,000 errors resulting from the updated file. The City GIS professional is confused and concerned that they've impacted live call routing.

   Response to hypothetical scenario:

10. NG9-1-1 Core Services Elements

Offeror shall provide a network or solution diagram that clearly depicts the Offeror's proposed transitional and end-state for the ESInet and the NGCS for the current City call center. The diagram should depict the City call center, and a second diagram should reflect the inclusion of neighboring independent jurisdiction with its own call handling equipment, GIS, voice logging, and call records management systems. There should be a diagram that depicts a proposed interconnection to another provider ESInet for the purposes of call transfers as well as redirect of all City incoming call traffic to a

remote call center that is not part of the City's ESInet. The following functional elements and services shall be included:

- LNG
- IP Carrier Connection
- LPG
- BCF
- ESRP
- PRF
- ECRF
- LVF
- SI
- LDB
- Discrepancy Reporting
- Logging and Recording
- Time Server

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

a) Legacy Network Gateway

1. The LNG is a signaling and media interconnection point between callers in legacy call-originating networks ("E9-1-1") and the NENA NG9-1-1 i3 architecture. As many communication service providers continue to use circuit switched SS7 message trunking for delivery of 9-1-1 calls to legacy SRs as well as deployed IP-based ESInets, there exists a need for the LGN. The LNG shall log all calls it receives and processes, and shall permit the uploading of daily log files to a network monitoring and management system for analysis. The conversion of SS7 messaging to IP-based communications may also be performed by Protocol Interworking Function devices that do not have interconnections to legacy ALI systems. Therefore, Offerors should be able to describe and diagram the ability to get ALI from carriers who are not providing PIDF-LO, especially those using SS7 connections, when there is no legacy ALI host. The LNG will need only exist while SRs are operating in the Commonwealth of Virginia and jurisdictions in North Carolina that abut the Tidewater region of Virginia. Offeror shall describe how solution shall interface directly with communication service providers who will interconnect directly to the City ESInet using SS7 with no PIDF-LO availability. The description should include how location information for these calls shall be maintained in a NG9-1-1 environment.

   The LNG shall allow for ad hoc uploads of log files for troubleshooting and incident response. All call activity on both the legacy side (Time-Division Multiplexing or TDM) and the IP side of the LNG shall be logged. The LNG shall have intrusion detection system ("IDS")/intrusion prevention system ("IPS") functionality to detect and mitigate distributed denial of service ("DDoS") attacks from both the TDM side and the IP side.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

Details to support the answer:

2. The LNG shall provide the capability to obtain location information from existing legacy ALI databases in order to define, create, populate, and send the correct PIDF-LO parameter to the correct ESRP or terminating PSAP.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

3. The LNG shall obtain location information and create the correct PIDF-LO message to pass on to the ESRP, as described within NENA-STA-010.2-2016.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

4. The LNG shall convert all incoming 9-1-1 calls to SIP calls in accordance with the SIP requirements of NENA-STA-010.2-2016. Any Offeror variations and/or non-compliance with the SIP requirements of NENA-STA-010.2-2016 must be identified and noted.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

5. The LNG external interfaces shall comply with respective NENA requirements.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

6. The LNG shall support obtaining the callback number associated with any pseudo ANI data that does not include the callback number. This may require the contractor to obtain the callback number from the wireless or Voice over Internet Protocol (“VoIP”) provider and may include additional recurring and non-recurring costs that are independent of this RFP. The contractor shall be responsible for all recurring and non-recurring costs associated with this requirement.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

Details to support the answer:

7. The LNG must facilitate logging of all significant events and 9-1-1 calls received and processed. Each call log shall contain all relevant parameters defined in Section 5.11.3 of NENA-STA-010.2-2016.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

8. All LNG logs files shall be capable of being extracted in near real time and shall be in a format suitable for importing into a spreadsheet or word processing program.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

9. The LNG solution must be deployed with the resiliency and redundancy to provide a minimum of 99.999 percent availability.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

10. The LSRG shall support star code transfers made by legacy PSAPs for calls destined for City PSAPs or to neighboring legacy PSAPs outside of the contractor's ESInet.

    ☐ Complies
    ☐ Complies Partially
    ☐ Complies with Future Capability
    ☐ Does Not Comply

    Details to support the answer:

11. Offeror shall describe how its LNG solution provides for LSRG functionality.

    ☐ Complies
    ☐ Complies Partially
    ☐ Complies with Future Capability
    ☐ Does Not Comply

    Details to support the answer:

12. Offeror shall provide the proposed locations for hosting the primary LNGs for serving the CITY OF VRIGINIA BEACH, including the data center tier level for the host sites.

    ☐ Complies
    ☐ Complies Partially
    ☐ Complies with Future Capability
    ☐ Does Not Comply

    Details to support the answer:

b) IP Direct Connection

1. The long-term evolution of NG9-1-1 will include the elimination of the current SRs. The communication service providers will then need to directly connect through to the ESInets for delivery of emergency calls. The LNG can accommodate all communication service providers who will continue to use SS7 carrier interconnection until the carrier completes its own migration to IP-based communication. However, as carriers migrate their networks, and as the PSTN migrates to IP, the ESInet solution must also be capable of direct IP connection from carriers. It should be noted that many carriers may choose to use aggregators for the delivery of emergency calls to ESInets. Interconnection points for carrier-direct connection should follow standard carrier interconnection practices in use in the industry today. Offerors will provide a minimum of two geographically diverse carrier interconnection points. These interconnection points shall be in the same Local Access Transport Areas (“LATAs”) as the ESInet hosted data centers. Offeror shall be responsible for the cross connection of direct carrier IP connection traffic to the Session Border Control (“SBC”) of the ESInet.

    ☐ Complies
    ☐ Complies Partially
    ☐ Complies with Future Capability
    ☐ Does Not Comply

    Details to support the answer:

2. IP interconnection from communication providers shall allow ready identification of carrier traffic to facilitate trouble resolution and location data issues. Offeror shall provide a high-level process for direct IP connection from carriers to include how carriers shall place interconnection requests and the approximate costs for interconnection.

    ☐ Complies
    ☐ Complies Partially
    ☐ Complies with Future Capability
    ☐ Does Not Comply

    Details to support the answer:

c) Legacy PSAP Gateway

1. The LPG is a signaling and media interconnection point between legacy PSAP CPE and the NGCS. The LPG allows for the transfer of calls from the ESInet to a PSAP that may not have upgraded its CPE to an i3-capable call handling system. The LPG also allows the legacy PSAP to transfer or alternately route legacy TDM calls to another PSAP on the ESInet.

    The LPG shall log all calls it receives and processes and shall permit the uploading of daily log files to a network monitoring and management system for analysis. The LPG shall allow for ad hoc

uploads of log files for troubleshooting and incident response in real time or near real time. All call activity on both the legacy ("TDM") side and the IP side of the LPG shall be logged. The LPG shall have IDS/IPS functionality to detect and mitigate DDoS attacks from the IP side.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

2. The LPG solution must be deployed with the resiliency and redundancy to provide a minimum of 99.999 percent availability.

   - ☐ Complies
   - ☐ Complies Partially
   - ☐ Complies with Future Capability
   - ☐ Does Not Comply

   Details to support the answer:

3. The LPG shall support a SIP interface toward the ESInet, as defined within NENA-STA-010.2-2016.

   - ☐ Complies
   - ☐ Complies Partially
   - ☐ Complies with Future Capability
   - ☐ Does Not Comply

   Details to support the answer:

4. The LPG shall support both CAMA and ALI interfaces toward the PSAP CPE that are compliant with the requirements of NENA-STA-010.2-2016.

   - ☐ Complies
   - ☐ Complies Partially
   - ☐ Complies with Future Capability
   - ☐ Does Not Comply

   Details to support the answer:

5. The LPG shall convert outbound call transfers to SIP in accordance with the requirements of NENA-STA-010.2-2016.

   - ☐ Complies
   - ☐ Complies Partially
   - ☐ Complies with Future Capability
   - ☐ Does Not Comply

   Details to support the answer:

6. The LPG shall support star codes as defined in NENA-STA-010.2-2016, with the exception that the star codes may be up to three digits in length.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

7. The LPG must facilitate logging of all significant events and 9-1-1 calls received and processed. Each call log shall contain all relevant parameters given in Section 5.11.3 of NENA-STA-010.2-2016.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

d) Border Control Function

1. The BCF shall provide logical network security functions between external networks and the ESInet and between the ESInet and City agency networks. The BCF is responsible for numerous functions, including the following:

- Border firewall
- VPN
- IDS/IPS
- SBC
- Opening and closing of pinholes
- Limiting access to critical components through the use of VLANs
- Call admission control
- Transcoding
- Signaling protocol normalization and interworking
- Network Address Translation ("NAT")
- Codec negotiation
- Support for QoS and priority markings
- Media proxy

The Offeror shall provide details, including drawings depicting how its proposed BCF meets or exceeds all functions listed above and the requirements described in NENA 08-003, as well as additional firewall requirements described in NENA 04-503 and NENA 75-001, or the next subsequent version of the NENA documents listed that are publicly available at the proposal release date.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

2. The BCF solution shall be deployed in a manner to achieve 99.999-percent availability.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

3. Management of the BCF shall include auditing of system log files for anomalies and processes for responding to and managing security incidents.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

4. The BCF must be capable of detecting when silence suppression is present in the 9-1-1 call, continuing to use silent suppression if detected, and not enabling silence suppression if it is not detected in the call.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

5. The BCF shall mediate all incoming 9-1-1 calls from VoIP providers to SIP calls in accordance with NENA-STA-010.2-2016. Any specific variations or non-compliance with this requirement must be identified and documented. The BCF shall support Back-to-Back User Agents (“B2BUAs”) for SIP.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

6. The BCF must provide the functionality to maintain logs of all 9-1-1 sessions and all additional BCF logging and recording requirements, as specified in NENA-STA-010.2-2016.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

7. The contractor’s BCF solution shall support transcoding of Baudot tones to real-time text, as described in IETF RFC 4103.

☐ Complies

☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

8. The Offeror shall provide details on how its proposed SBC will recognize that a NAT or Network Address and Port Translation ("NAPT") has been performed on Open Systems Interconnection ("OSI") Layer 3, but not above, and correct the signaling message for SIP.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

9. The Offeror shall provide details on how its proposed SBC shall enable interworking between networks using IPv4 and IPv6 through the use of dual stacks, selectable for each SBC interface, based on NENA-STA-010.2-2016. All valid IPv4 addresses and parameters shall be translated to/from the equivalent IPv6 values.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

10. The Offeror shall provide details on how its proposed SBC shall support SIP over the following protocols: Transmission Control Protocol ("TCP"), User Datagram Protocol ("UDP"), Transport Layer Security ("TLS") over TCP, and Stream Control Transmission Protocol ("SCTP"). Protocols supported must be selectable for each SBC interface to external systems. These transport layer protocols are generated and terminated at each interface to external systems.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

11. The Offeror shall provide details on how its proposed SBC shall be capable of populating the Layer 3 headers, based on call/session type (e.g., 9-1-1 calls) in order to facilitate priority routing of the packets.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

12. The Offeror shall provide details on how its proposed SBC supports encryption for calls that are not protected entering the ESInet, based on NENA-STA-010.2-2016.

    ☐ Complies
    ☐ Complies Partially
    ☐ Complies with Future Capability
    ☐ Does Not Comply

    Details to support the answer:

13. Offeror shall describe the functionality of the proposed BCF solution in sufficient detail to address the requirements outlined, with particular attention to the user interface and features, and the security aspects.

    ☐ Complies
    ☐ Complies Partially
    ☐ Complies with Future Capability
    ☐ Does Not Comply

    Details to support the answer:

14. The Offeror shall provide details, including drawings, depicting the different BCF elements that its proposed solution comprises. As part of the details, the Offeror shall provide all of the expected elements and/or interfaces to be provided by the City to the Offeror.

    ☐ Complies
    ☐ Complies Partially
    ☐ Complies with Future Capability
    ☐ Does Not Comply

    Details to support the answer:

e) Emergency Services Routing Proxy and Policy Routing Function

1. The ESRP routes a call to the next hop. It also evaluates the originating policy rules set for the queue the call arrives on, extracts the location of the caller from the SIP signaling, queries the ECRF for the nominal next hop route, evaluates the route based on policy rules and queue states of the downstream entity queues, and then forwards the call to the resulting next hop.

    ☐ Complies
    ☐ Complies Partially
    ☐ Complies with Future Capability
    ☐ Does Not Comply

    Details to support the answer:

2. The PRF is a required function of the ESRP. The ESRP interacts with the PRF to determine the next hop of a call or event. Before the ESRP sends the call to the next hop, it first queries the PRF to check the status of the next hop to determine if a unique routing rule, or policy, is in place that would direct the call to another location. The destination of the next hop is typically a queue. The PRF monitors the downstream queues of ESRPs for active understanding of the entity's queue status.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

3. The PRF shall allow defining policy rules for distributing a wide range of calls in an efficient manner. Offeror shall describe their solution's Policy Store and the PSAP's ability to affect change to the PRF. Please describe the user interface, the authentication process, and the types of policy rules available at the time of proposal submission (with examples for each), as well as those on the product roadmap. Roadmap items should include an estimated time of feature availability.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

4. A next-hop queue may be a URI that routes the call to an interactive multimedia response system (as described in IETF RFC 4240) that plays an announcement (in the media negotiated by the caller) and potentially accepts responses via Dual-Tone Multi-Frequency ("DTMF") signaling or other interaction protocols.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

5. The ESRP/PRF solution must be designed with resiliency and redundancy to provide a minimum of 99.999-percent availability.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

6. The Offeror shall provide an explanation of how its proposed ESRPs use the "options" transactions for maintaining "keep alive" between ESRPs, LNGs, LPGs, and session recording services.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

7. The upstream interface on the proposed non-originating ESRPs shall implement TCP/TLS, but must be capable of fallback to UDP, as described in NENA-STA-010.2-2016. SCTP support is optional. The ESRP shall maintain persistent TCP and TLS connections to the downstream ESRPs or User Agents ("UAs") that it serves.

   The Offeror shall provide detailed documentation describing how the non-originating ESRP interface supports TCP/TLS with fallback to UDP.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

8. The Offeror shall provide a description of how its ESRPs meet or exceed all functional requirements as defined in NENA-STA-010.2-2016, which are listed in the following table.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

Table 2. ESRP Functional Requirements

Requirement	NENA-STA-010.2-2016 Section	Complies	Complies Partially	Complies with Future Capabilities	Does Not Comply
4.10.4.8.1 Overview	5.2.1.1				
4.10.4.8.2 Call Queueing	5.2.1.2				
4.10.4.8.3 Queue State Event Package	5.2.1.3				
4.10.4.8.4 De-queue Registration Event Package	5.2.1.4				
4.10.4.8.5 Policy Routing Function	5.2.1.5				
4.10.4.8.6 ESRP Notify Event Package	5.2.1.6				
4.10.4.8.7 INVITE Transaction Processing	5.2.1.7				
4.10.4.8.8 BYE Transaction Processing	5.2.1.8				
4.10.4.8.9 CANCEL Transaction Processing	5.2.1.9				
4.10.4.8.10 OPTIONS Transaction Processing	5.2.1.10				
4.10.4.8.11 Upstream Call Interface	5.2.2.1				
4.10.4.8.12 Downstream Call Interface	5.2.2.2				
4.10.4.8.13 ECRF Interface	5.2.2.3				
4.10.4.8.14 Location Information Server ("LIS") Dereference Interface	5.2.2.4				
4.10.4.8.15 Additional Data Interfaces	5.2.2.5				

Requirement	NENA-STA-010.2-2016 Section	Complies	Complies Partially	Complies with Future Capabilities	Does Not Comply
4.10.4.8.16 ESRP, PSAP, Call-Taker State Notification and Subscriptions	5.2.2.6				
4.10.4.8.17 Time Interface	5.2.2.7				
4.10.4.8.18 Logging Interface	5.2.2.8				
4.10.4.8.19 Data Structures	5.2.3				
4.10.4.8.20 Policy Elements	5.2.4				
4.10.4.8.21 Provisioning	5.2.5				

f) Emergency Call Routing Function

1. The ECRF shall be designed according to NENA-STA-010.2-2016 and be implemented using diverse, reliable, and secure IP connections.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

2. Contractor shall supply an ECRF function that meets a minimum of 99.999-percent availability.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

3. Contractor providing an ECRF must ensure that it is accessible from outside the ESInet and that the ECRF permits querying by an IP client/endpoint, an LNG, an ESRP in a next generation emergency services network, or by some combination of these functions.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

4. An ECRF accessible inside an ESInet must permit querying from any entity inside the ESInet. ECRFs provided by other entities may have their own policies regarding who may query them.

   ☐ Complies
   ☐ Complies Partially

☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

5. An origination network may use an ECRF, or a similar function within its own network and at its own cost, to determine an appropriate route—equivalent to what would be determined by the authoritative ECRF—to the correct ESInet for the emergency call. Offeror shall describe the functionality of such an ECRF equivalent and document where this functional element resides. The contractor shall provide a SI to authorized entities, such as origination networks, to provide for replication of the ECRF for origination networks to determine the appropriate ESInet to route calls.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

6. The ECRF shall support a routing query interface that can be used by an endpoint, ESRP, or PSAP to request location-based routing information from the ECRF. Additionally, it must support both iterative and recursive queries to external ECRF sources.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

7. The ECRF must interface with the LoST protocol (as described in IETF RFC 5222) and support LoST queries via the ESRP, PSAP CPE, or any other permitted IP host.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

8. The proposed ECRF must allow for rate-limiting queries from sources other than the proposed ESRP(s) and provide logging of all connections, connection attempts, and LoST transactions.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

9. The ECRF must support:

- Logging of all connections, connection attempts, data updates, ECRF query results, and LoST transactions
- Updates from the SI in near real time with no degradation of LoST services
- Routing of calls based on geographic coordinates, geodetic shapes, and civic addresses
- Utilization of common GIS boundaries, including, but not limited to, PSAP, law enforcement, fire and emergency medical services ("EMS")
- Permitting of LoST queries for find service request association with each layer
- Compliance with NENA 02-010 and NENA 02-014
- Dynamic updates to GIS without disruption of the ECRF
- Validation of GIS updates before they are provisioned into the ECRF

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

10. Offeror shall define its method for: provisioning the ECRF; updating the ECRF (including the frequency of updates); validating data provisioning; performing error logging; performing gap and overlap analysis; and supporting LoST queries from ESRPs, the PSAP CPE, and other authorized hosts within the ESInet. The Offeror shall provide a clear description of the functionality of the ECRF, list features and capabilities, describe its error handling, default mechanisms and logging, and provide an overview of deployment recommendations to achieve 99.999-percent reliability.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

11. The City acknowledges that its ESInet will be part of an overall hierarchical plan that includes interconnectivity to other regions and State-level ECRFs. The Offeror shall provide details regarding its vision for how this interconnection will include replicas of ECRF/LVF at different levels of the hierarchy, as well as access/
origination networks.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

12. Offeror shall provide explanations of any tradeoffs between aggregations of data at higher level ECRFs versus the use of Forest Guides to refer requests between ECRFs that possess different levels of data. As part of that explanation, the Offeror shall provide details on how the appropriate ECR/LVF data should be provisioned for use in overload and backup routing scenarios, and any dependencies that might impact provisioning.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

g) Location Validation Function

1. An LVF is a LoST protocol server where civic location information for every call originating endpoint is validated against the SI-provisioned GIS data. The SI is responsible for provisioning and updating the information used for location validation in the LVF, which shall contain a standardized interface to the SI.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

2. The LVF must be available to validate civic locations at the time a wireline device is ordered (Service Order Interface [SOI] validation), when a nomadic device is connected to the network, and when a PSAP or other authorized entity makes a civic location validation request. The LIS/LDB shall be allowed to periodically revalidate the civic location information against the GIS data contained within the LVF.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

3. The LVF shall support all functionality as defined in NENA-STA-010.2-2016, shall be designed with resiliency and redundancy to provide a minimum of 99.999-percent availability and shall be provisioned with the same data as the ECRF.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

4. The Offeror should outline options for a public-facing LVF provisioned for use by service providers outside the ESInet.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

Details to support the answer:

5. Offeror shall describe the functionality of the proposed LVF solution in sufficient detail to address the requirements outlined, with particular attention to the arrangement of the proposed components, user interface and features, and security aspects.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

h) Spatial Interface

1. The SI is responsible for provisioning and updating authoritative GIS data to the ECRF and LVF. It is anticipated that, in the future, the City will require the PSAP tactical map display, computer-aided dispatch ("CAD") systems, and similar applications that consume GIS data will also receive updates via the SI. However, SI updates to these systems are not required at this time and this capability should not be priced in Offeror's cost proposal. GIS data provisioned by the SI must undergo data quality and data integrity checks to ensure the data complies with all applicable requirements of NENA 02-010, NENA 02-014, and Attachment B of NENA-STA-010.2-2016.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

2. The SI shall convert the GIS data meeting these requirements into the format (data structure and projection) used by the ECRF and LVF, in real time or near real time, using a Web feature service. The SI shall be able to provision and perform incremental updates, in near real time, to the ECRF, LVF, the map viewer service, the PSAP tactical map display, and similar applications that consume GIS data.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

3. Offeror shall describe the functionality of the proposed SI solution in sufficient detail to describe the validation of GIS data and data updates prior to their provisioning into the ECRF and LVF, along with the means of real-time or near real-time provisioning of incremental updates to the GIS data provisioned to the ECRF and LVF.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

4. Offeror shall describe its proposed workflow for receiving GIS updates from jurisdictions, to allow for a smooth transition from the existing processes that have been implemented during the preparation of the region's NG9-1-1 data by the jurisdictions. Offeror also must describe all security and monitoring aspects and any additional features supported by the proposed SI. Offeror shall also describe how they shall manage multiple GIS sources when there are several neighboring independent jurisdictions on the same ESInet as City. This description shall include how each entity will have a profile to provide GIS updates to the system. Offeror shall provide a high level process of overlap issue resolution.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

i) Location Database

1. A LDB serves as both a legacy ALI database and as an LIS in an i3 NG9-1-1 environment. The LDB retains all of the current information, functionality, and interfaces of today's ALI, but also can use the new protocols required in an NG9-1-1 deployment. The LDB supports the protocols for legacy ALI query and ALI query service, the protocols required to obtain information for wireless calls by querying the mobile positioning center ("MPC") or gateway mobile location center ("GMLC"), and the protocols required for i3 location information retrieval and conveyance, such as HELD or other proprietary protocols.

   The LDB must meet the following requirements:

   - Shall support all relevant sections of NENA 02-010, 02-011, 02-015, 04-005, 08-501, and 08-502 related to ALI DBMS
   - Shall be capable of assuming the role of a location DBMS as defined in the NENA NG9-1-1 Transition Plan Considerations (NENA INF 008.2-2013)
   - Shall support NENA standards (J-036, E2, E2+, NCAS, CAS)
   - Shall be able to provide LIS functionality and interfaces as defined in NENA-STA-010.2-2016
   - Shall be able to seamlessly interact with a NENA i3 ECRF, as described in NENA-STA-010.2-2016
   - Shall be able to dereference a location by reference, as defined in NENA-STA-010.2-2016
   - Shall be able to dereference requests for additional information, as defined in NENA-STA-010.2-2016
   - Shall be able to interface simultaneously with multiple wireless callers
   - Shall be able to interface simultaneously with multiple remote ALI databases
   - Shall automatically detect, import and validate customer records (SOI records)
   - Shall have the ability to be used simultaneously by both NG9-1-1-capable and E9-1-1-capable PSAPs
   - Shall allow different PSAPs to use different ALI formats based on individual needs
   - Shall use LVFs to validate civic addresses
   - Shall support location data formatting as defined in the NENA CLDXF
   - Shall periodically reevaluate the location information using LVF functions within the system

- Shall be able to communicate with NG9-1-1 functional elements using the HELD protocol
- Shall be able to provide a PIDF-LO based on both the wireless and VoIP E2 response
- Shall be able to dereference additional data request
- Shall consistently respond to all requests within 400 ms

Offeror shall describe the functionality of the proposed LDB, including additional features and capabilities, error handling, logging and deployment recommendations in sufficient detail to address the requirements outlined, with particular attention to the arrangement of the proposed components, user interface and features, and security aspects.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

2. The LDB shall support the integration of private ALI databases. This shall include any types of institutions as set forth in the Technical Requirements, Section B6 of this RFP. Offeror shall provide a description of how private or enterprise ALI database for stations behind a Private Branch Exchange ("PBX") system will be established migrated, updated, maintained, and partitioned from other users within the proposed NG9-1-1 system. The proposed solution shall be in alignment will all current NENA standards and industry practices for private switch ALI databases.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

j) Discrepancy Reporting

The Offeror shall provide details regarding its proposed solution's report functions for notifying agencies any time a discrepancy is detected with the BCF, ESRP, PRF, ECRF, LVF, and SI. As part of the detail, the Offeror shall explain how a report will be sent for the purpose of reporting the discrepancy to the City and any other independent participating jurisdictions.

Discrepancy reporting is outlined in Section 4.9 of NENA-STA-010.2-2016. Offeror shall describe the functionality of the proposed discrepancy reporting function in sufficient detail to address the requirements outlined, with particular attention to the user interface and features, and the security aspects.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

k) Event Logging and Management Information System

1. Extensive logging of NG9-1-1-related events, transactions, media, and operations is required. Logging includes all elements in the call flow including logging of events within ESInets, the NGCS, the PSAP, and related operations and is a standardized function used throughout ESInets, NG9-1-1 functional elements, and PSAPs. Logged events include ingress and egress to an ESInet, ingress and egress to a PSAP, all steps involved in call processing, and processing of all forms of media.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

2. Offeror shall describe how its event logging solution may integrate with each PSAP's call handling equipment to provide a complete, end-to-end view of a call, and/or describe how a PSAP can gain access to information in the event logging solution. Offeror shall describe requirements of the PSAP's call handling equipment, software license agreements, software licensing costs, and interfaces required to support integration with the Offeror's event-logging solution.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

3. Offeror shall describe how a PSAP can gain access to the event-logging solution to review recordings and run statistical and other Management Information System ("MIS") reports. Offeror shall describe retention periods associated with all logging records.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

4. Because logs may be subpoenaed and used as a source of information in legal proceedings, the logging systems shall be designed, proposed, and operated with legal defensibility of logged information taken into careful account. All log entries shall be accurately time stamped.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

5. The contractor's proposed logging solution must meet the requirements set forth in NENA-STA-010.2-2016.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

6. Contractor is responsible for any third-party software licensing costs and any other associated costs.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

7. Offeror shall describe the reports, MIS tools, and performance metrics made available to each PSAP that participates on the same ESInet as the City, the user interface for retrieving or receiving reports, and the ability to customize reports based on individual PSAP needs. The City desires reports and metrics that include, but are not limited to:

- Timing
  - Call delivery time
  - Call processing time between elements
- Volumes
  - Call volumes by call type
  - Alternate-routed calls
  - Text-to-9-1-1
  - All NGCS element usage volumes
- Bandwidth/Trunk Utilization
  - Calls per trunk
  - Trunk utilization
  - Circuit utilization
- Call Flows and Agent Activity
  - Call transfers
  - Call conferences
  - End-to-end call-flow analysis

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

l) Network Time Protocol and Time Source

1. Contractor shall provide redundant, resilient network-attached time sources (“master clocks”) capable of supplying standard time to all systems, network devices, and functional elements that comprise the ESInet and the NGCS.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

2. The master clock time source(s) shall be accessible to the PSAPs for synchronizing their call handling systems and other related systems. All systems, network devices, and functional elements shall support the use of the Network Time Protocol ("NTP") for maintaining system clock accuracy.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

m) NG9-1-1 Applications and Alarm Integration

1. NG9-1-1 provides for the capability to have alarm companies integrate directly with the ESInet and use the NGCS for routing of the alarm and its associated data. The City is interested in implementing such capabilities. As an optional service and priced separately, Offeror may describe its experience in integrating alarm and sensor data with its NGCS solution.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

2. As an optional service and priced separately, Offeror may describe other NG9-1-1 applications, additional data integrations, and personal safety applications that may be integrated with its NGCS solution.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

n) Message Session Relay Protocol Text Integration

The City PSAP has deployed short messaging service ("SMS") to 9-1-1 service with Comtech/TCS GEM 911. The text control centers ("TCCs") of both West and Comtech TCS are serving the region through a variety of direct MPLS network connectivity and Internet-based access. Offeror shall describe its ability to integrate existing Web-based and MSRP-integrated SMS to 9-1-1 and future Real Time Text ("RTT") into its ESInet. Offeror shall explain whether its solution supports location-by-reference and/or location-by-value. This requirement is for integration of text messaging with MSRP and not a requirement for procuring text services.

Offerors shall provide costs for MSRP integration with the NGCS in the Optional Costs Pricing table.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

11. Service Level Agreements

a) System Capacities and Performance

Offeror shall provide capacity levels of each element of the ESInet and the NGCS. This may be in terms of busy-hour calls, network bandwidth, or any other applicable measure. The proposed solution must be capable of handling current call volume plus 25-percent growth over the term of the contract. Offeror shall provide the incremental cost to handle 125 percent of current call volume in the Optional Pricing table. Offeror shall specify lead times required to increase capacities on each element of the ESInet and the NGCS.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

b) System Performance

1. **Network Latency.** Offeror shall specify the guaranteed maximum latency across its backbone network under a full-load condition and include how that information will be gathered, calculated, and provided to the City.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

2. **Point of Presence ("POP") to POP.** Offeror shall specify the guaranteed maximum latency from interconnection facility (aka, point of presence or POP) to interconnection facility, and include how that information will be gathered, calculated, and provided to the City.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

3. **POP to Endpoints.** Offeror shall specify the guaranteed maximum latency from interconnection facilities to the network interface device located at the entrance to the customer's premises and include how that information will be gathered, calculated, and provided to the City.

   ☐ Complies

☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

4. **Packet Loss.** Offeror shall specify the guaranteed maximum end-to-end packet loss across its network. This specification also shall include any loss characteristics associated with another carrier's network or any applicable wireless links, including how that information will be gathered, calculated, and provided to the City.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

5. **Network Traffic Convergence.** Offeror shall specify convergence protocols and the estimated or guaranteed network convergence time (<54 milliseconds [ms]) of IP traffic at any point within the proposed solution, including how convergence information will be gathered, calculated, and provided to the City.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

6. **Mean Time to Repair.** Offeror shall specify the mean time to repair ("MTTR") characteristics of its proposed solution. These specifications shall reflect the end-to-end solution, as well as components or subsystems that are subject to failure. Offeror shall include how MTTR information will be gathered, calculated, and provided to the City.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

7. **Mean Time Between Failures.** Offeror shall specify the mean time between failures ("MTBF") characteristics of its proposed solution. These specifications shall reflect the end-to-end solution, as well as components or subsystems that are subject to failure. Offeror shall include how MTBF information will be gathered, calculated, and provided to the City.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

8. **System Availability.** Offeror shall specify the service level offered as a percentage of time when the service is available and the maximum period of total outage before remedies are activated. Availability is defined as MTBF/(MTBF+MTTR). Offeror shall include how system availability information will be gathered, calculated, and provided to the City.

    ☐ Complies
    ☐ Complies Partially
    ☐ Complies with Future Capability
    ☐ Does Not Comply

    Details to support the answer:

9. **End-of-Support Equipment.** Contractor shall proactively replace any hardware that has reached end of support ("EOS") no later than 90 days prior to the manufacturer's EOS date.

    ☐ Complies
    ☐ Complies Partially
    ☐ Complies with Future Capability
    ☐ Does Not Comply

    Details to support the answer:

10. **Remedies.** Offeror shall define the financial and operational remedies to the City and its respective specified agencies for each event in which the above system performance service levels are not maintained.

    ☐ Complies
    ☐ Complies Partially
    ☐ Complies with Future Capability
    ☐ Does Not Comply

    Details to support the answer:

c) SLAs for Incident Management

It is expected that the contractor will have processes and procedures for supporting a NOC/ SOC that can rapidly triage calls. In the absence of reasonably proposed processes, the contractor shall meet, at a minimum, the following requirements for tracking, responding to, and reporting on network and system outages or failures:

- Severity Level 1 incidents responded to within 30 minutes and resolved within 4 hours of detection
- Severity Level 2 incidents responded to within 30 minutes and resolved within 8 hours of detection
- Severity Level 3 incidents responded to within 8 hours and resolved within 48 hours
- Severity Level 4 incidents responded to within 16 hours and resolved within 96 hours

These severity levels are defined as follows:

Severity 1 Incident
An incident shall be categorized as a "Severity 1 Incident" if the incident is characterized by the following attributes: the incident (a) renders a business-critical system, service, software, equipment or network component unavailable or substantially unavailable, or seriously impacts normal business operations, in each case prohibiting the execution of productive work; and (b) affects either (i) a group or groups of people, or (ii) a single individual performing a critical business function.

Severity 2 Incident
An incident shall be categorized as a "Severity 2 Incident" if the incident is characterized by the following attributes: the incident (a) does not render a business-critical system, service, software, equipment or network component unavailable or substantially unavailable, but a function or functions are not available, substantially available, or functioning as they should, in each case prohibiting the execution of productive work; and (b) affects either (i) a group or groups of people, or (ii) a single individual performing a critical business function.

Severity 3 Incident
An incident shall be categorized as a "Severity 3 Incident" if the incident is characterized by the following attributes: the incident causes a group or individual to experience an incident with accessing or using a system, service, software, equipment or network component or a key feature thereof and a reasonable workaround is not available, but does not prohibit the execution of productive work.

Severity 4 Incident
An incident shall be categorized as a "Severity 4 Incident" if the incident is characterized by the following attributes: the incident may require an extended resolution time, but does not prohibit the execution of productive work and a reasonable workaround is available.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

d) Outage Notification and Reason for Outage Report

1. Contractor shall comply with all applicable FCC rules throughout the term of the services contract.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

2. Contractor shall notify the City jurisdictions and/or its designee within 30 minutes of discovering an outage that may impact 9-1-1 services. At the time of initial notification, the contractor shall convey all available information that may be useful in mitigating the effects of the outage, as well as a name, telephone number, ticket or reference number, and email address at which the service provider can be reached for follow-up. The contractor is responsible for coordinating data gathering, troubleshooting, and reporting on behalf of its suppliers.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

3. Contractor shall communicate any additional material information to the City or its designee no later than 2 hours after the initial contact and at intervals no greater than 2 hours thereafter until normal

9-1-1 service is restored. This information shall include the nature of the outage, its best-known cause, the geographic scope of the outage, the estimated time for repairs, and any other information that may be useful to the management of the affected facility.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

4. Following the restoration of normal 9-1-1 service, contractor shall provide a Reason for Outage ("RFO") Report/Root Cause Analysis to the City jurisdictions and/or its designee, no later than 30 days after discovering the outage. Offeror shall describe its compliance with the notification and reporting requirements stated above. Offeror shall describe the NOC/SOC tools and techniques at its disposal to ensure its various suppliers perform troubleshooting and post-event analysis and provide associated reports.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

e) SLA Reporting

Offeror shall provide a detailed description of how it measures and reports incidents, including immediate notifications and regularly scheduled reports. The mechanism shall deliver SLA results to the City and its designees on a monthly basis. The report shall include all performance items identified in the contractor's proposal and documented in contract negotiations.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

f) SLA Violations

An SLA violation shall have occurred whenever:

- The contractor fails to meet any single performance level.
- The average of any single performance item over the preceding 2-month period fails to meet the service level. This is an "early warning" of an unacceptable trend.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

g) Incident Severity Level 1 and 2 Credits

Contractor shall provide a monetary credit of the Monthly Recurring Fee ("MRF") to the City each event in which service levels are not maintained. The City expects that all of the contractor's network devices and services will perform at a level equal to 99.999 percent uptime measured on a rolling 12-month calendar. Failure to meet service levels shall be measured per service-affecting outage. Offeror shall include how uptime information will be gathered, analyzed, and provided to the City.

Contractor shall meet the following requirements for tracking, responding to, and reporting on network and system outages or failures:

- Severity Level 1 incidents responded to within 30 minutes and resolved within 4 hours of detection
- Severity Level 2 incidents responded to within 30 minutes and resolved within 8 hours of detection

The following severity levels are defined as follows:

Severity 1 Incident
An incident shall be categorized as a "Severity 1 Incident" if the incident is characterized by the following attributes: the incident (a) renders a business-critical system, service, software, equipment or network component unavailable or substantially unavailable, or seriously impacts normal business operations, in each case prohibiting the execution of productive work; and (b) affects either (i) a group or groups of people, or (ii) a single individual performing a critical business function.

Severity 2 Incident
An incident shall be categorized as a "Severity 2 Incident" if the incident is characterized by the following attributes: the incident (a) does not render a business-critical system, service, software, equipment or network component unavailable or substantially unavailable, but a function or functions are not available, substantially available, or functioning as they should, in each case prohibiting the execution of productive work; and (b) affects either (i) a group or groups of people, or (ii) a single individual performing a critical business function.

For Severity Level 1 and 2 incidents, a 10-percent credit of the MRF shall be due to the City and its respective agencies, as applicable when the initial period of resolution is exceeded. If the resolution period length of time doubles, then the credit shall increase to 20 percent of the MRF. If the resolution period length of time quadruples the initial period, then 50 percent of the MRF shall be credited. The credited amount shall be included on the invoice of each affected City jurisdiction the month immediately following the violation.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

12. PSAP Interfaces and Backroom Equipment Requirements

1. The PSAP call interface is a SIP call interface as described in NENA-STA-010.2-2016. The geolocation header, call information headers and other headers shall be the same as described in NENA-STA-010.2-2016. The call will be routed, using normal RFC 3261 procedures, to the URI obtained from the ESRP's PRF. See NENA-STA-010.2-2016, Section 5.6 for other information on the PSAP interface.

   ☐ Complies

☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

2. Contractor's solution shall support PSAP interfaces specified in NENA-STA-010.2-2016, Section 4.1, including the following:

- SIP call interface
- SIP subscribe and notify
- Support for Web services
- Support for HELD and LoST queries and responses
- Support for placing abandoned call return
- Support of SIP call transfer, call bridging, and call conferencing
- Support for all baseline media and multimedia as described in NENA-STA-010.2-2016, Section 4.1
- Support for ad hoc location validation
- Support for queries to and responses from additional data repositories
- Support for NTP time services interface, accurate to 1 millisecond
- Support for logging of all calls, queues, upstream element states, and incoming calls and their associated media
- Support for TLS
- Support for the NENA/APCO EIDD—use throughout document
- Support for SMS, instant messaging, and star code equivalent transfers
- Support for test calls

Offeror shall describe the functionality of the PSAP interfaces in sufficient detail to address the requirements outlined, with particular attention to the user interface, additional features, and security aspects.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

Remote PSAP Footprint Description (if applicable):

13. Migration Plan Options

1. Offeror shall describe its proposed migration plan to the NG9-1-1 system from the existing E9-1-1 system, highlighting any potential disruption to existing operations at the City primary PSAP, as well as any costs the Offeror is relying on the PSAP or NGCS project to cover. Also, any specific dependencies the Offeror has for a successful implementation that are seen as PSAP responsibilities should be explained clearly. The City seeks a migration plan that provides for the most cost-effective migration while ensuring the integrity of the region's mission-critical 9-1-1 services. Offeror shall describe how its solution minimizes reliance on legacy SRs and ALI database services. This detail shall include ingress network design, ESInet design, data center

build plans, a clear project schedule of activities (including Gantt charts), example test plans, process audits, risk mitigation plans, and staffing plans. This migration plan should comport with the Virginia Information Technology Agency ("VITA") NG Migration proposals for the Commonwealth of Virginia

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

2. The Offeror shall provide a Master Project Plan ("MPP") that depicts the major sequencing of project activities and the timeline for each activity at the Work Breakdown Structure ("WBS") level. Within 60 days of successful contract award, the contractor shall develop an implementation plan for each jurisdiction's individual PSAPs, identifying any unique characteristics and tasks that are required for integration with each PSAP's call handling system, and the contractor's NGCS solution, using aforementioned i3 protocols such as SIP, PIDF-LO, LoST, HELD, and HTTP (GET).

   - ☐ Complies
   - ☐ Complies Partially
   - ☐ Complies with Future Capability
   - ☐ Does Not Comply

   Details to support the answer:

3. Offeror shall provide examples of where this migration methodology has been successfully deployed in the past.

   - ☐ Complies
   - ☐ Complies Partially
   - ☐ Complies with Future Capability
   - ☐ Does Not Comply

   Details to support the answer:

4. Offeror shall describe any steps that the City PSAP should take to streamline the migration project, with descriptions of required resources and details regarding what is required versus optional.

   - ☐ Complies
   - ☐ Complies Partially
   - ☐ Complies with Future Capability
   - ☐ Does Not Comply

   Details to support the answer:

14. Project Management and Ongoing Client Management Services

1. Offeror shall describe its project management methodology and support structure. Please describe the daily, weekly, and monthly interactions during the migration.

   - ☐ Complies
   - ☐ Complies Partially

☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

2. Offeror shall identify by name and provide resumes for the specific project team that will manage the migration. Project Managers with industry standard certifications, for example Project Management Institute PMP certification, are preferred.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

3. Offeror shall provide a description of each team member's role and their anticipated amount of time dedicated to the project. Offeror shall describe key team members' experience in managing and implementing projects of similar size and scope.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

4. Contractor shall not change key staff during the course of the project without mutual agreement with the City. The City desires for Offerors to bring key staff members to oral presentations, if invited.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

5. Offeror shall describe the post-deployment client management service, including client management reports, executive briefings, and the fielding of ad hoc support requests.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

15. Training

1. Contractor shall provide comprehensive training for the implementation process and ongoing maintenance of the NGCS and ESInet. Training should also be available on an annual basis or when key city personnel changes require it.Offeror shall describe its training program, including, but not limited to, the following topics: trouble reporting, help desk Web interface, PRF policy store interface, SI discrepancy reporting, LDB data management, and service monitoring tools.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

2. Offeror shall describe the types of attendees required to attend training, training curriculum, number of training attendees included in the proposed price, and the duration of the training program per attendee (expressed in hours per day and number of days), as well as the location of the training and whether such training is available online. Preference is given to training that can be conducted within the City. Examples of proposed training plans and training materials are desired.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

16. Service, Repair and Advance Replacement

As this is a service-based offering, the City shall not be responsible for the replacement and maintenance of hardware and software required to provide the ESInet and the NGCS. Contractor must resolve all faults or malfunctions at no additional cost to the City.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

17. Software Release Policy

18. Scheduled Releases

1. Offeror shall describe the frequency of scheduled software releases, the feature release testing process, and the decision-making processes involved in deciding what features and defect resolutions to include in a scheduled release. Offeror agrees that documentation of release notes shall be available to City thirty (30) days before implementation. This documentation should detail the deployment process and timeline for scheduled and maintenance releases. Also, a description of how releases shall be tested within the ESInet, including call handling equipment.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

2. Offeror shall explain how it replicates the client environment for software release testing in order to provide assurances that future software releases will not negatively impact PSAP operations.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

19. Maintenance Releases

1. Offeror shall describe the frequency of defect resolution software releases, as well as the decision-making processes involved in selecting which software defects to fix.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

2. The contractor shall provide the City with access to the contractor's defect tracking system in order for the City to track the progress of defect resolutions.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

3. The contractor shall provide a detailed description of the software defect tracking process and provide training to City staff prior to Final Acceptance Testing.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

4. Offeror shall describe how software defects are aged. For example, a minor problem (from the Offeror's perspective) can become a major or critical problem if not resolved in a timely manner. For example, a column of numbers in an MIS report may not total properly. While this certainly is not a service-affecting problem, it does make the PSAP administrator's job more difficult if these totals have to be maintained separately and totaled manually. Using this example, the Offeror shall describe in detail how/when this minor problem gets scheduled or automatically escalated, and the feedback mechanism in place for keeping the City PSAP informed.

   ☐ Complies
   ☐ Complies Partially
   ☐ Complies with Future Capability
   ☐ Does Not Comply

   Details to support the answer:

20. Documentation

The contractor shall provide the City PSAP with pertinent documentation for the ESInet and NGCS and update the City PSAP as configurations change over the term of the contract. The required documentation shall include the following:

- Customized migration plan
- Escalation procedures
- Circuit identification
- Single points of failure
- Network path diversity drawings into each data center
- Network path diversity drawings into each PSAP
- PSAP backroom as-built drawings
- PSAP demarcation point drawings
- System Design Document with high level schematic of interconnection to Network Nodes
- All user interface training and reference materials

The contractor shall provide all documentation in agreed-upon soft copy format. Additionally, access to documentation on a contractor-hosted Web-portal is desired.

☐ Complies
☐ Complies Partially
☐ Complies with Future Capability
☐ Does Not Comply

Details to support the answer:

IV. GENERAL TERMS AND CONDITIONS

A. LICENSING, SUPPORT, AND MAINTENANCE PERIOD

The City intends to contract for these references services for a contract period of five (5) years. For the purposes of software licensing and support, any resulting Contract may be extended upon mutual written agreement of both parties for ten (10) additional one-year periods based upon the same terms and conditions set forth in the Contract.

B. RENEWAL

The City may consider price adjustments, after Year 5 of contract term. Contractor shall provide to the City a written request for any such increases. Such requests shall be addressed to the Issuing Office. A minimum thirty-(30)-day advance notice period shall be required for such requests.

Requests for price increases adjustments are subject to the review and approval of the City Purchasing Agent. Any increase in cost shall not increase by a greater percentage than the percentage change of the Other Goods and Services category of the CPI-W section of the Consumer Price Index published by the United States Department of Labor during the previous twelve months or 5% whichever is lower.

Requests for price increases adjustments are subject to the review and approval of the City Purchasing Agent.

C. TERMINATION WITH CAUSE/DEFAULT/CANCELLATION

In the event that Contractor shall for any reason or through any cause be in default of the terms of this Agreement, the City may give Contractor written notice of such default by certified mail/return receipt requested at the address set forth in association contract or in Contractor's RFP response.

Unless otherwise provided, Contractor shall have thirty (30) days from the date such notice is mailed in which to cure the default. Upon failure of Contractor to cure the default, the City may immediately cancel and terminate this Agreement as of the mailing date of the default notice.

Upon termination, Contractor shall withdraw its personnel and equipment, cease performance of any further work under the Agreement, and turn over to the City any work in process for which payment has been made.

In the event of violations of law, safety or health standards and regulations, this Agreement may be immediately cancelled and terminated by the City and provisions herein with respect to opportunity to cure default shall not be applicable.

D. NONDISCRIMINATION

Employment discrimination by Contractor shall be prohibited. During the performance of this Agreement, Contractor agrees as follows:

1. Contractor will not discriminate against any employee or applicant for employment because of race, religion, color, sex, national origin, age, disability, or any other basis prohibited by state law relating to discrimination in employment, except where there is a bona fide occupational qualification/ consideration reasonably necessary to the normal operation of Contractor. Contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices setting forth the provisions of this nondiscrimination clause.

2. Contractor, in all solicitations or advertisements for employees placed by or on behalf of Contractor, will state that Contractor is an equal opportunity employer.

3. Notices, advertisements and solicitations placed in accordance with federal law, rule or regulations shall be deemed sufficient for the purpose of meeting the requirements of this section.

4. Contractor will include the provisions of the foregoing Sections 1, 2, and 3 in every subcontract or purchase order of over $10,000, so that the provisions will be binding upon each subcontractor or Contractor.

E. DRUG FREE WORKPLACE

During the performance of this Agreement, Contractor agrees as follows:

1. Contractor will provide a drug-free workplace for Contractor's employees.

2. Contractor will post in conspicuous places, available to employees and applicants for employment, a statement notifying employees that the unlawful manufacture, sale, distribution, dispensation, possession, or use of a controlled substance or marijuana is prohibited in Contractor's workplace and specifying the actions that will be taken against employees for violations of such prohibition.

3. Contractor will state in all solicitations or advertisements for employees placed by or on behalf of Contractor that Contractor maintains a drug-free workplace.

4. Contractor will include the provisions of the foregoing Sections 1, 2, and 3 in every subcontract or purchase order of over $10,000, so that the provisions will be binding upon each subcontractor or Contractor.

F. FAITH BASED ORGANIZATIONS

The City of Virginia Beach does not discriminate against Faith-Based Organization.

G. COMPLIANCE WITH IMMIGRATION LAWS

Contractor does not currently, and shall not during the performance of this Agreement, knowingly employ an unauthorized alien, as defined in the federal Immigration Reform and Control Act of 1986.

H. BUSINESS ENTITY REGISTRATION

Foreign and domestic businesses authorize to transact business in the Commonwealth. The Contractor shall be registered and authorized to transact business in the Commonwealth as a domestic or foreign business entity if so required by Title 13.1 or Title 50 or as otherwise required by law. The Contractor shall submit proof of such registration to the City. Additionally, the Contractor shall not allow its existence to lapse or its certificate of authority or registration to transact business in the Commonwealth, if so required under Title 13.1 or Title 50, to be revoked or canceled at any time during the term of the contract.

I. COMPLIANCE WITH ALL LAWS

Contractor shall comply with all federal, state and local statutes, ordinances, and regulations now in effect or hereafter adopted, in the performance of scope of work set forth herein. Contractor represents that it possesses all necessary licenses and permits required to conduct its business and will acquire any additional licenses and permits necessary for performance of this Agreement prior to the initiation of work.

J. VENUE

Any and all suits for any claims or for any and every breach or dispute arising out of this Agreement shall be maintained in the appropriate court of competent jurisdiction in the City of Virginia Beach, or the U.S. District Court for the Eastern District of Virginia, Norfolk District.

K. AGREEMENT INTERPRETED UNDER LAWS OF VIRGINIA

This Agreement shall be deemed to be a Virginia contract and shall be governed as to all matters whether of validity, interpretations, obligations, performance or otherwise exclusively by the laws of the Commonwealth of Virginia, and all questions arising with respect thereto shall be determined in accordance with such laws. Regardless of where actually delivered and accepted, this Agreement shall be deemed to have been delivered and accepted by the parties in the Commonwealth of Virginia.

L. BUSINESS LICENSE REQUIREMENT

If the Contractor is a business, located in the City of Virginia Beach or at any time during the performance of this Agreement obtains situs for purposes of business license taxes, it shall be unlawful for such business to conduct or engage in such business, trade or occupation without having first obtained the proper license from the Commissioner of the Revenue of the City, and the Contractor covenants that it has a business license where one is required to perform this Agreement.

M. INDEPENDENT CONTRACTOR

The Contractor shall agree and covenant that it is and shall be at all times, an independent contractor, and as such, shall have and maintain complete control over all of its employees and operations. Neither

the Contractor nor anyone employed by it shall be, represent, act, purport to act, or be deemed to be an agent, representative, employee or servant of the City. Nothing in this section shall be deemed to absolve or otherwise limit the Contractor's liability and responsibility to safely and correctly perform its duties under this Agreement.

N. REPRESENTATION REGARDING CITY EMPLOYMENT; CONFLICT OF INTEREST:

Contractor represents at the time of contracting and through the pendency of this Agreement that no one with an ownership interest in the Contractor or the Contractor's corporate entity, if applicable, or other employee of the Contractor is also an employee of the City of Virginia Beach, specifically in the City Department initiating or overseeing this Agreement. Contractor further represents that no individual with an ownership interest in the Contractor or the Contractor's corporate entity, if applicable, or other employee has a spouse, other relative or person who resides with the individual that is currently an employee of the City of Virginia Beach, specifically in the City Department initiating or overseeing this Agreement. Should the Contractor have reasonable belief of a possible conflict of interest, that issue should immediately be brought to the attention of the City's Purchasing Division for review.

O. INTEGRATION/MERGER

This Agreement and any appendices attached hereto constitute the entire agreement of the parties and supersedes all prior agreements, understandings and negotiations, whether written or oral, between the parties. This Agreement may not be modified, except in a writing signed by both parties that is expressly stated to be an amendment hereto.

P. SEVERABILITY

The provisions of this Agreement shall be deemed to be severable, and should any one or more of such provisions be declared or adjudged to be invalid or unenforceable, the remaining provisions shall be unaffected thereby and shall remain in full force and effect.

Q. WAIVER

No failure of the City to exercise any right or power given to it by law or by this Agreement, or to insist upon strict compliance by Contractor with any of the provisions of this contract, and no custom or practice of the parties at variance with the terms hereof, shall constitute a waiver of the City's right to demand strict compliance with the terms of this Agreement.

R. INTERPRETATION

Whenever the context hereof shall require, the singular shall include the plural, the plural the singular, and the use of any gender shall be applicable to all genders.

S. DESCRIPTIVE HEADINGS

The descriptive headings appearing in this Agreement are for convenience only and shall not be construed either as a part of the terms, covenants, and conditions hereof or as an interpretation of such terms, covenants, and conditions.

T. NON-APPROPRIATION

It is understood and agreed between the Parties hereto that the City shall be bound and obligated hereunder only to the extent that the funds shall have been appropriated and budgeted for the purpose of this Agreement. In the event funds are not appropriated and budgeted in any fiscal year for payments due under this Agreement, the City shall immediately notify Contractor of such occurrence and this Agreement shall terminate on the last day of the fiscal year for which appropriations were received without penalty or expense to the City of any kind whatsoever.

U. ASSIGNMENT OF AGREEMENT

The Contractor shall not, without the prior written consent of the City, assign, delegate, or otherwise transfer, in whole or in part, the Agreement or any of the Contractor's rights or obligations arising hereunder. The City may, in its sole discretion, consent or decline to consent to any such assignment, delegation, or transfer, or may give its conditional consent thereto. In the event the City conditionally consents to such an assignment, delegation, or transfer, such consent may, without limitation, be conditional upon Contractor's remaining fully and unconditionally liable to the City for any breach of the terms of this Agreement by Contractor's transferee and for any damage or injury sustained by a third party or parties as a result of the intentional act or omission, negligence, or breach of warranty by Contractor's transferee.

V TERMINATION WITHOUT CAUSE

The City may at any time, and for any reason, terminate this Agreement by written notice to Contractor specifying the termination date, which shall be not less than thirty (30) days from the date such notice is mailed. Notice shall be given to Contractor by certified mail/return receipt requested at the address set forth in this Agreement.

In the event of such termination, Contractor shall be paid such amount as shall compensate Contractor for the work satisfactorily completed, and accepted by the City, at the time of termination.

IF THE CITY TERMINATES THIS AGREEMENT WITH CAUSE, CONTRACTOR SHALL WITHDRAW ITS PERSONNEL AND EQUIPMENT, AND CEASE PERFORMANCE OF ANY FURTHER WORK UNDER THIS AGREEMENT.

W HOLD HARMLESS/INDEMNIFICATION

It is understood and agreed that Contractor hereby assumes the entire responsibility and liability for any and all damages to persons or property caused by or resulting from or arising out of any act or omission on the part of Contractor, its subcontractors, agents or employees under or in connection with this Agreement or the performance or failure to perform any work required by this Agreement. Contractor agrees to indemnify and hold harmless the City and its agents, volunteers, servants, employees and officials from and against any and all claims, losses, or expenses, including reasonable attorney's fees and litigation expenses suffered by any indemnified party or entity as the result of claims or suits due to, arising out of or in connection with (a) any and all such damages, real or alleged, (b) the violation of any law applicable to this Agreement, and (c) the performance of the work by Contractor or those for whom Contractor is legally liable. Upon written demand by the City, Contractor shall assume and defend at Contractor's sole expense any and all such suits or defense of claims made against the City, its agents, volunteers, servants, employees or officials.

X INSURANCE

Contractor agrees to secure and maintain in full force and effect at all times during the term of this Agreement, the following policies of insurance:

1. Workers' Compensation Insurance of not less than $500,000.

2. Comprehensive General Liability Insurance, including contractual liability and products and completed operations liability coverages, in an amount not less than one million dollars ($1,000,000) combined single limits ("CSL"). Such insurance shall name the City of Virginia Beach as an additional insured.

3. Automobile Liability Insurance including coverage for non-owned and hired vehicles in an amount not less than one million dollars ($1,000,000) combined single limits.

4. Errors and Omissions (Professional Liability) Insurance at limits not less than one million dollars ($1,000,000).

All policies of insurance required herein shall be written by insurance companies licensed to conduct the business of insurance in Virginia, and acceptable to the City, and shall carry the provision, that the insurance will not be cancelled or materially modified without thirty days (30) prior written notice to the City. In certain cases, where coverage is unavailable through licensed carriers, certificates of insurance written by a Surplus Lines Carrier authorized by the Virginia State Corporation Commission to transact the business of insurance in Virginia and acceptable to the City of Virginia Beach may be approved. Contractor shall list the City of Virginia Beach as an additional insured, and furnish the City with certificate of insurance showing Contractor's compliance with the foregoing requirements.

Y NOTICE

All notices and requests required or permitted hereunder shall be sent by United States certified mail, return receipt requested and to be effective, shall be postmarked no later than the final date for giving of such notice; or such notices may be sent by commercial messenger service, in which event, to be effective, such notices shall be delivered to a commercial messenger service not later than the final date for giving such notice.

Notices for the City of Virginia Beach shall be addressed as follows:

Darla L. Smith
Purchasing Division
2388 Liberty Way
Virginia Beach, VA 23456

Notices for Contractor shall be addressed in accordance with address provided in signed contract, or address shown in the Contractor's RFP submittal.

Such addresses may be changed at any time and from time to time by like written notice given by either party to the other.

Z OFFSET/SETOFF

The City may withhold the payment of any claim or demand by any person, firm or corporation against the City until any delinquent indebtedness or other liability, including taxes, due to the City from such person, firm or corporation shall first have been settled and adjusted.

AA. AUDITS

The City shall have the right to audit all books and records (in whatever form they may be kept, whether written, electronic or other) relating or pertaining to this Agreement (including any and all documents and other materials, in whatever form they may be kept, which support or underlie those books and records), kept by or under the control of Contractor, including, but not limited to those kept by Contractor, its employees, agents, assigns, successors and subcontractors. Contractor shall maintain such books and records, together with such supporting or underlying documents and materials, for the duration of this Agreement and for at least three years following the completion of this Agreement, including any and all renewals thereof. The books and records, together with the supporting or underlying documents and materials shall be made available, upon request, to the City, through its employees, agents, representatives, contractors or other designees, during normal business hours at Contractor's office or place of business in Virginia Beach, Virginia. In the event that no such location is available, then the books and records, together with the supporting or underlying documents and records, shall be made available for audit at a time and location in Virginia Beach, Virginia, which is convenient for the City.

This paragraph shall not be construed to limit, revoke, or abridge any other rights, powers, or obligations relating to audit which the City may have by state, city, or federal statute, ordinance, regulation, or agreement, whether those rights, powers, or obligations are express or implied.

BB. COOPERATIVE PROCUREMENT

This Agreement was awarded in accordance with Section 2.2-4304 of the Virginia Public Procurement Act ("VPPA), and in accordance with the City of Virginia Beach's Procurement Code. The procurement was conducted on behalf of the City and other public bodies. Therefore, pursuant to Code Section 2.2-4304, other public bodies and agencies shall have the right to utilize the provisions of the contract. However, when other public bodies and agencies utilize the contract, Contractor must establish a separate contractual relationship between it and the other party. Under no circumstances shall the City of Virginia Beach be a party to or incur any obligations or responsibilities, contractual or otherwise, in association with these contractual agreements between the Contractor and another public body or agency.

CC. SUBMISSION AND DISPOSITION OF CONTRACTUAL CLAIMS

Prompt knowledge by the City of an existing or impending claim for damages or other relief may alter the plans, scheduling, or other action of the City and/or result in mitigation or elimination of the effects of the claim. Therefore, a written statement providing the City with notice of the Contractor's intention to file a claim which (i) describes the act or omission by the City or its agents that the Contractor contends caused it damages or entitles it to other relief; and (ii) provides a description of the nature and amount of the claim. Such written statement shall be submitted to the City within 20 days of the time of the occurrence or beginning of the work upon which the claim is based; provided, however, if such damage is deemed certain in the opinion of the Contractor to result from its acting on an order from the City, it shall immediately take written exception to the order. For purposes of this provision, "claim" shall include, without limitation, any request for an increase in the contract price or time and any request for equitable adjustment. Submission of a notice of claim as specified shall be mandatory, and failure to submit such notice shall be a conclusive waiver to such claim for damages or other relief by the Contractor. Neither an oral notice or statement, nor an untimely notice or statement will be sufficient to satisfy the requirements herein.

The City will review the claim and render a final decision in writing within thirty (30) days of receipt of Contractor's written request for a final decision. Such decision shall be final and binding to the fullest extent allowed by law.

DD. PAYMENTS TO SUBCONTRACTORS

In accordance with Title 2.2, Chapter 43, Article 4 of the Code of Virginia (Virginia Public Procurement Act), the Contractor shall make payment to all subcontractors, as defined in the Code, within seven (7) days after receipt of payment from the City; or, shall notify the City and the subcontractor in writing of the intention to withhold all or part of the amount due with the reason for nonpayment. In the event payment is not made as noted, the Contractor shall pay interest at the rate of one percent (1%) per month, unless otherwise provided in the contract, to the subcontractor on all amounts that remain unpaid after seven (7) days except for the amounts withheld as provided herein.

These same requirements shall be included in each subcontract and shall be applicable to each lower-tier subcontractor. The Contractor shall provide the City with its social security number or federal taxpayer identification number prior to any payment being made under this Agreement.

The Contractor's obligation to pay an interest charge to a subcontractor pursuant to the payment clause in this section may not be construed to be an obligation of the City. A contract modification may not be

made for the purpose of providing reimbursement for such interest charge. A cost reimbursement claim may not include any amount for reimbursement for such interest charge.

EE. SUBCONTRACTORS

The use of subcontractors and the work they are to perform shall receive prior written approval of the contract administrator. The Contractor shall be solely responsible for all work performed and materials provided by subcontractors. The Contractor shall be responsible for the liability of subcontractors for the types and limits required of the Contractor.

V. SPECIAL TERMS AND CONDITIONS

A. PAYMENT SCHEDULE

1. Payment for nonrecurring charges for services rendered by the Contractor shall be billed in accordance with the following schedule:

    a. 5% upon execution of a master service agreement, finalized schedule and implementation plan, and Statement of Work

    b. 25% of the contract amount after all City customizations and configurations have been delivered and installed in a test environment

    c. 35% of the contract amount after the product with City customizations is installed, configured in the production environment

    d. 35% of the contract amount 30 days after final system acceptance

2. Payment on invoices shall be Net 30 days after receipt of a properly submitted and approved by City invoice.

B. MODIFICATION

There may be no modification of any resulting Contract, except in writing, executed by the authorized representatives of the City and the Contractor.

C. COMPANY PERSONNEL STANDARDS

1. Personnel shall be trained/qualified to perform requested services. If any of the successful Offeror's personnel are not satisfactory in the performance of services to be furnished hereunder in a proper manner and satisfactory to the City, the Offeror shall remove any such personnel and replace them with satisfactory personnel.

2. Offerors shall use all reasonable care, consistent with its rights to manage and control its operations, not to employ any persons or use any labor or have any equipment or permit any condition to exist which shall or may cause or be conducive to pose any liability to the general public as well as any activity to be construed as a nuisance. The City retains the right to require the successful Offeror to halt all work activities until such conditions are resolved.

D. CLAIMS FOR EXTRA COMPENSATION

If Contractor encounters work and services not included in the resulting Contract or any supplement thereto but which in the opinion of Contractor is necessary for the successful completion of the Contract and requires extra compensation, Contractor shall, before it begins the work on which it bases its claim, promptly notify the City in writing of its intention to perform the work and to make claim for extra compensation. Notification by Contractor under the terms of this paragraph shall not be construed as

proving the validity of the claim. No claim for extra compensation will be filed or considered unless notification is given as herein set forth.

Upon notification, the City shall promptly review any claim for extra compensation. If a claim is accepted by the City, it shall be paid as extra work in accordance with the terms of a supplemental agreement executed by the parties before such work is begun.

The amounts claimed as extra compensation by Contractor shall be separately itemized, become a part of the claim, and serve as documentation thereto. The amounts itemized shall be in sufficient detail to enable the City to analyze the need for the extra work and the costs claimed for the work.

E. COPYRIGHT/PATENT INDEMNITY

In the event any third party shall claim that the manufacture, use and sales of the goods supplied under the contract constitute an infringement of any copyright, trademark or patent, the Contractor shall indemnify the City and hold the City harmless from any cost, expense, damage or loss incurred in any manner by the City on account of any such alleged or actual infringement.

F. LICENSE

1. The Contractor grants the City a perpetual, non-exclusive, nontransferable license to use the Software, for internal data processing operations of the City and its agencies, for the applicable maximum number of designated users.

2. The Contractor grants the City rights to make a reasonable number of copies or translate the Licensed Programs in machine readable or printed form solely for a development environment, a test environment, a train environment, and archive, emergency backup, and disaster recovery purposes.

3. The Contractor grants the City rights to use the Licensed Programs in a back-up environment in the event the City's production environment is temporarily inoperable.

4. The Contractor grants the City rights to make a reasonable number of copies of documentation solely for use of the City and its agencies. The City agrees to reproduce all copyright notices.

5. The City agrees not to cause or permit the reverse engineering, disassembly, decompilation or recompilation of the Software Products.

6. The Contractor and its subcontractors shall retain all title, copyright and other proprietary rights in the Software Products and all modifications, enhancements and other derivative works of the Software Products unless developed by the City or otherwise agreed upon by the parties.

7. There shall be no licensing restrictions to granting access to citizens and business partners via the internet.

8. The City retains ownership of all data and rights to extract data into non-proprietary formats.

City current system data shall remain the sole property of the City of Virginia Beach. Therefore, all tools and capabilities native to the database/OS environment, either Oracle/SQL Server, Unix/Windows, as proposed, shall be available to the City to allow for full access to that data. All tables, layouts, queries, stored procedures, XML schema and other content developed to support the operation of the database and the FOIA solution in the City's environment become the property of the City, and shall be available to the appropriate City personnel as needed and upon request. Database query, extract and data download capabilities into external formats such as MS Excel and Access or any other machine readable format shall be completely operational and available for appropriate City personnel to access.

The above is not meant to include proprietary programs or other intellectual property unique to the Offeror's solution. However, such claim to proprietary content cannot intrude on the City's right to access its data without undue interference or additional cost. Data owned by the City of Virginia Beach may not be used by the Offeror for any purposes without the express written consent of the appropriate City representative.

G. WARRANTY

Contractor shall warrant that the System shall be substantially free from programming errors and shall conform to the standards and system requirements set forth in the contract and that the services to be performed by the Contractor shall be performed in a timely and professional manner by qualified personnel. The terms of this warranty shall expire five (5) years after the date of Acceptance of the System.

The Contractor shall respond to requests for warranty service in accordance with Section 11 of the Technical Requirements, Service Level Agreements. The Contractor warrants and represents that the System shall be free of any willfully introduced computer virus or any other similar harmful, malicious or hidden programs or data, and the Contractor shall indemnify and hold harmless the City from (i) any costs or damages awarded against the City in connection with any such virus, programs or data (ii) the cost of debugging any virus and (iii) cost of alternative processing while debugging is under way.

H. STANDARDS

1. All proposed products and services shall comply with City of Virginia Beach standards as documented in ***Attachment B, City of Virginia Beach Computing Environment and Information Technology Standards*.**

2. The solution shall integrate with the existing communication, network and workstation environment at the City of Virginia Beach.Beach.

3. All proposed products and services shall comply with applicable federal, state, and local statutes.

I. SUBCONTRACTORS

1. While the Contractor may utilize the products and services from several suppliers, the Contractor shall be solely responsible for the successful completion of the implementation.

2. Deliverables shall address all components of the solution, including those provided by subcontractors and third party providers.

J. PROJECT TEAM MEMBERS

1. The Offeror's implementation Project Manager and Technical Lead are expected to coordinate and participate in all activities related to Offeror demonstrations, if shortlisted.

2. The Offeror's implementation Project Manager and Technical Lead are required to attend and participate in all contract negotiation activities.

3. The Contractor shall indicate the percentage of time the proposed project manager shall work on-site for the duration of the project.

4. Key members of the Contractor's project team shall be subject to approval by the City. Support personnel proposed shall have the necessary level of training and experience with the application

suite to ensure that the City is receiving expert-level support. The Offeror may be requested to provide the City with a listing of all certificates, training courses and other relevant evidence to document the level of expertise of proposed support personnel.

5. During the project, the Contractor shall replace key team members within 30 days when notified by City that the member is unacceptable.

6. Key personnel, including the Project Manager and Technical Lead are required to staff the project from project inception to three months after whole system acceptance. Offeror shall describe (if any) role the Technical Lead or other key personnel will take in subsequent support of system.

7. The City prefers the Offeror's Project Manager to be PMP certified. Further, the Offeror's Project Manager and Technical Lead will not be removed without prior approval by the City of Virginia Beach Project Manager.

8. In the unlikely event that the Offeror requests any key Offeror staff be removed prior to the above time period, a mutually agreeable detailed transition plan shall be developed for the City which includes a minimum 45 day succession plan before the Offeror's Project Manager will be released, at no additional cost to the City. The purpose of this plan is to ensure minimal disruption to the project. The City will have the unilateral ability to reject any replacement key staff for any reason.

K. SECURITY

1. All Contractor and Subcontractor personnel with access to the data shall sign confidentiality agreements.

2. All software products shall execute without hardware security access devices (e.g., security dongles).

3. All electronic storage media (floppy disks, Zip disks, CD-ROMs, DVDs, flash memory cards, USB drives, etc.), tapes, hard drives, embedded memory systems (routers or switches), shall be cleared or destroyed before any transfer, disposal, or surplus occurs. Media that contains sensitive data (privacy, financial, personal health information ("PHI"), or criminal or civil investigation results shall be destroyed before disposal.

4. All Contractor and Subcontractor personnel with access to the data shall authorize the City to conduct criminal background investigations.

    a. Criminal Background Check – Due to the sensitive nature of the areas to which the Successful Offeror's staff will have access, the City is requiring a criminal background check on staff assigned to the project, including any and all sub-contractor personnel. This includes any personnel who will either be on site or who has access to city data that is not normally available to public scrutiny.

    b. Personnel will be required to submit to a Virginia/Federal criminal background checks for all project specific personnel prior to commencement of work.

    c. Successful Offeror will be required to submit Form PD-150 on all project personnel. (To be provided upon notification by the City of an Offeror's being shortlisted)

    d. The City will be responsible for any and all costs associated with obtaining said background checks.

    e. The City will not accept personnel having a criminal record without the prior written approval of the City's Chief Information Officer or his designee.

f. The City's Contract Administrator will return to the Contractor the list of names with either "permitted" or "not permitted" to indicate personnel who can have the access.

g. Confidentiality Agreement – The successful Offeror will be required to submit completed Attachment G - Confidentiality Agreements for all personnel assigned to the project.

L. PRODUCT DOCUMENTATION

1. The Contractor shall provide the system, system administration and user documentation for the base product in an electronic format.

2. The Contractor shall include system flow charts, program narratives, data dictionaries, file layouts, database schemas and logical entity relationship diagrams in the documentation.

3. The Contractor shall maintain and keep current the documentation in a timely manner and provide it to the City at no additional cost. This should be presented quarterly if system designs changes so warrant.

4. The Contractor shall modify the documentation to reflect customizations for the City.

5. The Contractor shall provide hardware and system software documentation including a System Design document.

6. The Contractor shall provide workflow diagrams for GIS components of the solution.

M. PRODUCT MODIFICATIONS

1. The Contractor shall include all modifications necessary for legislated changes occurring within the project timeframe at no additional cost to the City.

2. During the project, the Contractor shall perform analysis of project Change Requests to provide cost estimates at no additional cost to the City.

N. PRODUCT TRAINING

The Contractor shall provide a training plan that includes:

1. Training of 125 end users
2. Training of 20 members of administrative / technical staff
3. Use of the City's training facilities
4. The minimum number of training hours included in base package
5. The trainer staff and hours
6. The training materials in both hard and soft copies
7. The size and assumed skill levels of each group and the functional responsibilities covered in each session
8. Assessment after training is complete of skill levels of all trainees and recommendations for additional training

O. PRODUCT TESTING

1. The Contractor shall conduct a product integration test prior to cut over of live emergency call traffic to ensure the delivered product modifications and product interfaces work to specifications and do not adversely impact the system as a whole.

2. The Contractor shall fix errors identified during testing and deliver the fixes to the City at no additional cost.

3. The selected contractor will be expected to provide the delineated testing support. Testing will be separated into three phases:

   - System Testing
   - End-User Acceptance Testing
   - Post-Production Deployment Testing

   System Testing will be initiated to verify the setup and configuration of the proposed software product. During System Testing, City developed test cases and test scripts will be exercised, updated as appropriate and finalized.

   End-User Acceptance Testing will follow System Testing and will continue until all test scripts and test cases have been executed acceptably by the end-user community. At the conclusion of End-User Acceptance Testing a 'Go/No Go' production deployment decision will be made.

   The Post-Production Monitoring will begin after production deployment. Metrics for reliability will be by mutual agreement between the City of Virginia Beach and the successful Offeror.

P. PRODUCTION DEPLOYMENT

1. The Contractor shall provide on-site support during production deployment.

2. During production deployment, Contractor resources shall provide support outside of normal working hours at no additional cost.

Q. POST INSTALLATION SUPPORT/RELIABILITY TEST PERIOD

1. The Contractor shall provide immediate support for production critical issues to the City during the first sixty (60) days of operation starting the 1st day of production use of the software product

2. During the Post-Production Deployment Reliability Test Period, the system must perform fully without degradation of any kind in order for the reliability test to be satisfied. If any major defects or numerous minor defects are discovered, the reliability test period shall be terminated and the Offeror shall resolve any and all issues. Once all issues have been addressed, the Post-Production Deployment Reliability Test Period will recommence from the beginning.

3. The Contractor shall provide the City immediate support for production critical issues during the Post-Production Deployment Reliability Test Period.

4. The Contractor shall perform a post-production deployment review of all product defect reports and develop an action plan to address these issues.

R. FINAL SYSTEM ACCEPTANCE

1. The project is not considered complete and the Contractor shall not be released from their obligations until a whole system acceptance test is conducted and the City formally accepts the system in writing.

2. The City and the Contractor will perform a whole system acceptance test to confirm that the system performs to a level that meets the City's expectations prior to cutting over live traffic to the new system.

3. Final system acceptance shall not occur until all deliverables have been received and approved for production.

4. Final system acceptance shall also not occur until the solution has been in production for thirty (30) days with no significant issues. During this period the Contractor shall provide post implementation support services.

5. At the successful completion of the reliability test period, the City shall issue the conditional acceptance certificate. At the end of the successful completion of both the reliability test period, data conversion (if required), and the whole system acceptance test, the City shall issue the final acceptance certificate.

S. PRODUCT ON-GOING SUPPORT AND MAINTENANCE

The Contractor shall enter into a multi-year maintenance and support agreement to include:

1. Access to the Contractor's product support help desk 24x7 including national and VA state holidays.
2. Responses to inquiries regarding operation and use of the product.
3. Product fixes as they become available.
4. Regular product releases.
5. Documented procedures for installation of software.
6. Certification within six months that the current or a new release of the product can be operated with new major versions of operating system software and database management system software.
7. Certification within 4 months that the current version or a new release of the product can be operated with service packs for operating system software and database management system software.

VI. SPECIAL INSTRUCTIONS TO THE OFFEROR

A. CONTRACT ADMINISTRATOR

Whenever used in the Request for Proposal and for purposes of any notices under this contract, the Contract Administrators shall be as described below:

During implementation:

City of Virginia Beach
Brittany Jennings
Department of Information Technology
4801 Columbus Street, Suite 202
Virginia Beach, VA 23462

B. PRE-PROPOSAL CONFERENCE

A pre-proposal conference will at 11:30 AM EST on January 18, 2019, at the Purchasing Division's conference room located at 2388 Liberty Way Drive, Virginia Beach, Virginia 23456. The City will conduct a tour of both the Emergency Communications and Citizen Services Center and the City's Emergency Communications Back Up Center as part of the pre-bid conference for in-person attendees. A conference bridge will also be set-up; reference the cover page of this document for information. The purpose of the conference is to clarify and answer any questions associated with the solicitation. Any changes determined necessary as a result of this conference or any other source which may affect the responses to the solicitation shall be formally addressed by the Issuing Office via addenda. Attendance of this conference is not mandatory, but is strongly advised. Interested participants may call in at (757) 385-1785 (local number) and 1-(877) 222-2238 (long distance number). Access Meeting ID 5940.

VII. GENERAL SUBMITTAL TERMS AND CONDITIONS

A. DEFINITIONS OF TERMS

The following definitions of terms are used herein:

1. The term “City” refers to the City of Virginia Beach.

2. The term “Offeror” refers to the person, firm, or company that provides a proposal in response to this Request For Proposal (“RFP”) and who may or may not be successful in achieving an opportunity to negotiate for the final award of a contract.

3. The term “Contractor” means the Offeror to which the contract will be awarded. References to the Contractor in this RFP shall also apply in full to any subcontractor for the named Contractor.

B. SUBMITTAL OF PROPOSALS

1. The proposal and required copies shall be placed in a sealed envelope or package that shall be identified with the Request for Proposal’s item number, the Date and Time of closing, and the name and address of the Offeror. The Offeror’s Cost Proposal should be submitted in a separate sealed envelope and identified as such.

2. An original and seven (7) copies of each proposal shall be submitted. In addition, the Offeror shall provide their proposal in electronic/digital read only format on a flash drive. The original proposal should be clearly marked “ORIGINAL” on its outside cover.

3. All proposals shall be received and time-stamped in the office location described below no later than 3:00 p.m. local time, February 6, 2019. Proposals received after the specified date and time (time-stamped 3:01 p.m. or later) shall not be considered and shall be returned unopened to the Offeror.

4. Issuing Office:

   City of Virginia Beach
   Attention: Darla L. Smith
   2388 Liberty Way
   Virginia Beach, VA 23456
   (757) 385-4438

5. Proposals received by telephone, telegraph, facsimile or any other means of electronic transfer shall not be accepted.

6. An Offeror receiving a Request For Proposal from a source other than the Issuing Office or DemandStar by Onvia, should contact the Issuing Office to become an Offeror Of Record before submitting its proposal.

C. EXAMINATION

Offeror shall carefully examine the contents of this Request for Proposal and any subsequent addenda.

D. QUESTIONS

1. Questions concerning this solicitation may be made in writing. Questions should be emailed to the Issuing Office not less than **five (5) working days prior to the date of the Pre-Bid conferenc**e of the Request for Proposal.

2. Any material changes to the solicitation document will be addressed by issuance of a written addendum to all Offerors of Record that will become part of the proposal documentation.

3. Oral instructions do not form a part of the proposal documents.

4. The Offeror shall check with the Issuing Office within forty-eight (48) hours prior to proposal closing to secure any addenda affecting bidding.

E. CONDITIONS OF WORK

Each Offeror shall inform himself/herself fully of the conditions relating to the project and the employment of labor therein. Failure to do so will not relieve a successful Offeror of his obligation to furnish all materials and labor necessary to carry out the provisions of this agreement.

F. ANTICOLLUSION/NONDISCRIMINATION//DRUG-FREE WORKPLACE FORM

The attached Anticollusion/Nondiscrimination/Drug-Free Workplace form incorporated herein (page 2) should be executed and returned with the proposal documents.

G. SUBCONTRACTING PARTICIPATION PLAN FORM

Offeror shall execute and return the Subcontracting Participation Plan (CVAB-GS1) Page 3, of this Request for Proposal. If the form is not returned with the Offeror's proposal, the form will be provided within three (3) days after notification that the Offeror has been shortlisted for further evaluation by the City.

H. GOOD-FAITH EFFORTS – CERTIFIED SMALL, WOMAN, MINORITY, SERVICE DISABLED VETERAN OR EMPLOYMENT SERVICES ORGANIZATION

It is the policy of the City of Virginia Beach to encourage the participation of Small, Woman, Minority and Service Disabled Veteran owned businesses, or Employment Services Organizations in its procurement processes. The City expects Offerors to embrace these goals to the maximum extent possible. To the extent practicable, the submitted proposal should provide for the fair inclusion of these businesses in their proposal. The businesses shall by certified by the Virginia Department of Small Business and Supplier Diversity. A list of certified businesses may be found at the following link:

Virginia Department of Small Business & Supplier Diversity - Small, Women and Minority ("SWaM") Contractors Search

I. PROPOSAL BINDING FOR ONE HUNDRED TWENTY (120) DAYS

The Offeror agrees that this proposal shall be good and may not be withdrawn for a period of one hundred twenty (120) calendar days after the scheduled closing time for the Request For Proposal.

J. PROPRIETARY INFORMATION

Offerors are advised that Section 2.2-4342 of the Code of Virginia, i.e., the Virginia Public Procurement Act, shall govern public inspection of all records submitted by the Offeror. Specifically, if Offeror seeks to protect any proprietary data or materials, pursuant to Section 2.2-4342, **Offeror shall (i) invoke the protections of this section prior to or upon submission of the data or other materials, (ii) identify the data or other materials to be protected, and (iii) state the reasons why protection is needed.** Furthermore, the Offeror shall submit proprietary information under separate cover, and the City reserves the right to submit such information to the City Attorney for concurrence of the Offeror's claim that it is in fact proprietary. References may be made within the body of the proposal to proprietary information; however, all information contained within the body of the proposal not labeled proprietary or

otherwise not meeting all three of the requirements of Section 2.2-4342 shall be public information in accordance with State statutes.

K. PROPOSAL COSTS

Prospective Offerors shall be responsible for all costs incurred in the development and submission of a proposal. The City assumes no contractual obligation as a result of the issuance of this RFP, the preparation or submission of a proposal by an Offeror, any cost associated with interviews and travel, or any other Offeror cost involved in a response.

L. EXCEPTIONS

Proposals should be as responsive as possible to the provisions stated herein, however, an Offeror may take exceptions to the provisions without their proposal being disqualified. During the evaluation process, the City will consider whether the impacts of any such exceptions are positive or negative. The Offeror should clearly indicate when exceptions or deviations are being taken and state the reason why. Notwithstanding the above, proposals received late shall be rejected.

M. AWARD

The award of a contract shall be the sole discretion of the City. The award shall be based upon the evaluation of all information as the City may request. The City reserves the right to accept or reject any or all proposals in whole or in part and to waive any informalities in the bidding. Further, the City reserves the right to enter into any contract deemed to be in the best interest of the City.

N. FRAUD, WASTE AND/OR ABUSE

The City of Virginia Beach is committed to eliminating fraud and maintaining a highly ethical environment throughout our organization. The City's Fraud, Waste and Abuse Prevention Program, coordinated by the Office of the City Auditor, consists of a Fraud Hotline, web site, awareness training and investigation services. While this program is designed to assist City employees, departments, agencies and programs in preventing and detecting incidents of fraud, waste and abuse in the City of Virginia Beach, it is also available to City contractors for this same purpose. This program focuses on dishonest acts by City employees or its contractors. Therefore, if you suspect any Fraud, Waste and/or Abuse regarding a City employee or contractor please call the Fraud Hotline at (757) 468-3330.

O. PUBLIC NOTICE OF AWARD OR DECISION TO AWARD

Public notice of the award or the announcement of the decision to award shall be provided by posting the appropriate notice on the "bid board" located in the Issuing Office, posting notice with DemandStar by Onvia, and mailing the notice to the Offerors who submitted proposals in response to the solicitation.

P. PREPARATION GUIDELINES

For consideration, all proposals should be as responsive as possible to the solicitation. In order to adequately evaluate the proposals, all Offerors shall use the following format:

1. Experience **(25 Points)**

   Offeror shall provide a concise description of their work experiences as it relates to the scope of work outlined herein. Said description shall include, but not be limited to:

   a. The Offeror's established experience record in providing comparable services.
   b. The number of years the Offeror has been providing these types of services.
   c. A minimum of three (3) references for whom the Offeror has provided services comparable to those described in this RFP.

(1) For each reference, the Offeror shall include:
   (a) Name of firm
   (b) Address of firm
   (c) Name, title, e-mail address, phone and fax of a contact for the firm
   (d) Version and platform the reference is currently running
   (e) Number of years Offeror has served the firm and
   (f) Brief summary of scope of services provided.

(2) The Offeror shall provide the following types of references if available:
   (a) One reference should be a city or county of similar size and complexity.
   (b) One reference should be an organization of similar size and complexity operating with live traffic at least one (1) or more years.

(3) The Offeror may provide one or more references of third party providers of integration services with experience integrating the Offeror's product with other applications. Describe how the integration is accomplished. Provide how many integrated instances of the proposed solution are currently in place.

2. Capability and Skills **(25 Points)**

The Offeror shall provide a description of the qualifications and skills of the organization and personnel who shall be responsible for performance of the services. Such description shall, at a minimum, include the following:

a. A description of the Offeror's company history and current operating characteristics to include the number of years in business, philosophy, ownership, number of employees, organizational chart, annual sales, and geographic coverage.

b. A description of the Offeror's financial stability and other resources that most adequately ensures the delivery of acceptable services to the City. The Offeror shall indicate the type of organization they represent, i.e., individual, partnership or corporation. If the Offeror represents a corporation or partnership, the names of the President, Vice-President, Secretary, Treasurer and all principals or partners shall be listed.

c. The Offeror should provide financial statements - i.e., audited annual financial reports, for the previous three (3) years.

   A listing of the personnel that will be assigned to the project along with a summary of their qualifications and specific responsibilities for the project.

d. Resources available to the organization for performance of the contract; including major subcontractors, work they will perform, approximate percentage of the total contract, term of agreement between Contractor and the subcontractor, and whether they are SWAM certified by the Virginia Department of Small Business and Supplier Diversity ("SBSD"). Resources for locating SBSD SWAM certified businesses may be found at the following link:

   Virginia Department of Small Business and Supplier Diversity

e. A graphical representation of the proposed project team structure including Contractor, City, and subcontractor team members

f. A description of the Offeror's business operations and history of providing similar services to public safety entities.

g. Evidence of the Offeror's ability to obtain the required and insurance.

h. A description of the Offeror's software development methodology and tools

i. A description of the Offeror's approach to providing non-standard and customized reports and interfaces

j. A description of the Offeror's testing methodology and tools

k. A description of the Offeror's approach to volume testing and evaluation of performance

l. A description of the Offeror's change management methodology and tools

m. A description of the Offeror's project management methodology

n. A description of the Offeror's ability to remotely access the proposed system in the development or test environment if it resides in the City's facilities. State the method(s) of remote site connectivity that would be used.

o. A description of the Offeror's ability to respond to requirement changes. Also, does the Offeror have sufficient manpower to make modifications to the software as required in a timely manner?

3. Services to be Provided **(25 Points)**

The Offeror shall provide a description outlining the services to be performed. Such description shall provide the Offeror's understanding of the overall effort and the project's goals and objectives. Include a description of how the Offeror plans on accomplishing the efforts identified in this RFP and all attachments. Include the following items in your response.

a. Services

Provide a detailed description/discussion of how your organization will provide services identified in the RFP. Include the following items in your response.

1) The Offeror's understanding of the project

2) A listing of all major tasks or services to be performed by the Offeror and the deliverables associated to each

3) A proposed implementation schedule delineating activities and resources required from contract award through final system acceptance. Include Gantt charts (or similar graphic depiction) to illustrate phases, activities, tasks, comments, milestones, decision points and deliverables. The actual project plan and schedule will be jointly developed by the Contractor and the City after the contract is awarded.

4) Completed **Attachment H –** Requirements Compliance Summary Matrix

5) A listing of City management, technical and user responsibilities, positions and expertise needed to conduct the project

5) A listing of the City positions, roles and expertise needed to operate, input data, export data and retrieve information from the System in the production environment

6) A detail listing of any assistance and materials the Offeror will require the City to furnish

7) Provide a detailed description/discussion of how your organization will address the project team participation requirements.

8) A description of the proposed data modeling and configuration services associated with any implementation of a GIS component or interface, including an example data model diagram.

9) A description of the fit analysis services proposed by the Offeror

10) A description of the recommended training associated with the proposed solution. Include the number of training hours in the base package and a discussion of the location of any training that cannot occur at City training facilities. Assume training is for 125 end users and 20 members of technical staff.

11) A description of conversion services proposed by the Offeror. Describe the City work effort associated with the conversion of data.

12) A description of the installation services proposed by the Offeror including assistance with preparing the environment, installing/upgrading the hardware and software, and placing the solution in operational mode

13) A description of the type of support proposed by the Offeror for the System, including problem response times and problem escalation procedures.

b. Other

1) Itemized responses to the database questions in **Attachment E, *Database* Questionnaire**, if applicable.

2) Provide itemized responses to each of the system requirements listed in Attachment H - Requirements Compliance Summary Matrix.

3) A description of application hosting options which the Offeror may be able to provide.

4) A listing of any exceptions taken to the provisions of this RFP, exclusive of exceptions taken to any liability provisions contained in the solicitation. The Offeror shall state any exceptions, to any liability provisions contained in the RFP, in writing within three business days of being notified that they have been selected for the negotiation phase of the procurement process.

4. Price **(25 Points)**

The Offeror shall provide a detailed description of the total cost to provide the proposed solution using Attachment F - ESInet Services and Software Investment Summary in a separate sealed envelope.

In the *Ongoing Costs* section, please identify modifications that are not included in standard annual maintenance and specify the associated maintenance/support costs. Please identify each item in the section *Other Ongoing Costs* (specify), e.g. Interface to XYZ System Annual Maintenance $nnn.nn.

Q. PROPOSAL OPENING

At the time specified, the proposals received timely shall be opened. Only the names of the Offerors submitting proposals shall be read aloud. No other information will be provided at that time.

R. EVALUATION

The City shall select two (2) or more Offerors deemed to be fully qualified and best suited among those submitting proposals on the basis of the factors listed below:

1. Offeror's experience in providing the services requested.
2. Offeror's capability and skill to perform the services.
3. Responsiveness of the written proposal to the purpose and scope of work.
4. Price. The total cost to provide the services described in the proposal.

The City intends to use a numerical scoring system in the evaluation, and such scoring will be 25 points assigned to each of the four factors listed above: Experience; Capability and Skill; Services to be Provided; and Price. There is a maximum of 100 possible points. A further description of these factors is set forth in Section VI.P ("Preparation Guidelines").

S. PRESENTATION/DEMONSTRATION

The City shall request the "short-listed" Offerors to conduct presentations/ demonstrations of the Offeror's proposed System's features and capabilities. Offeror presentations/ demonstrations shall be at a City site, at a date and time mutually agreed to between the City and Offeror, and shall be at the Offeror's expense.

T. NEGOTIATIONS

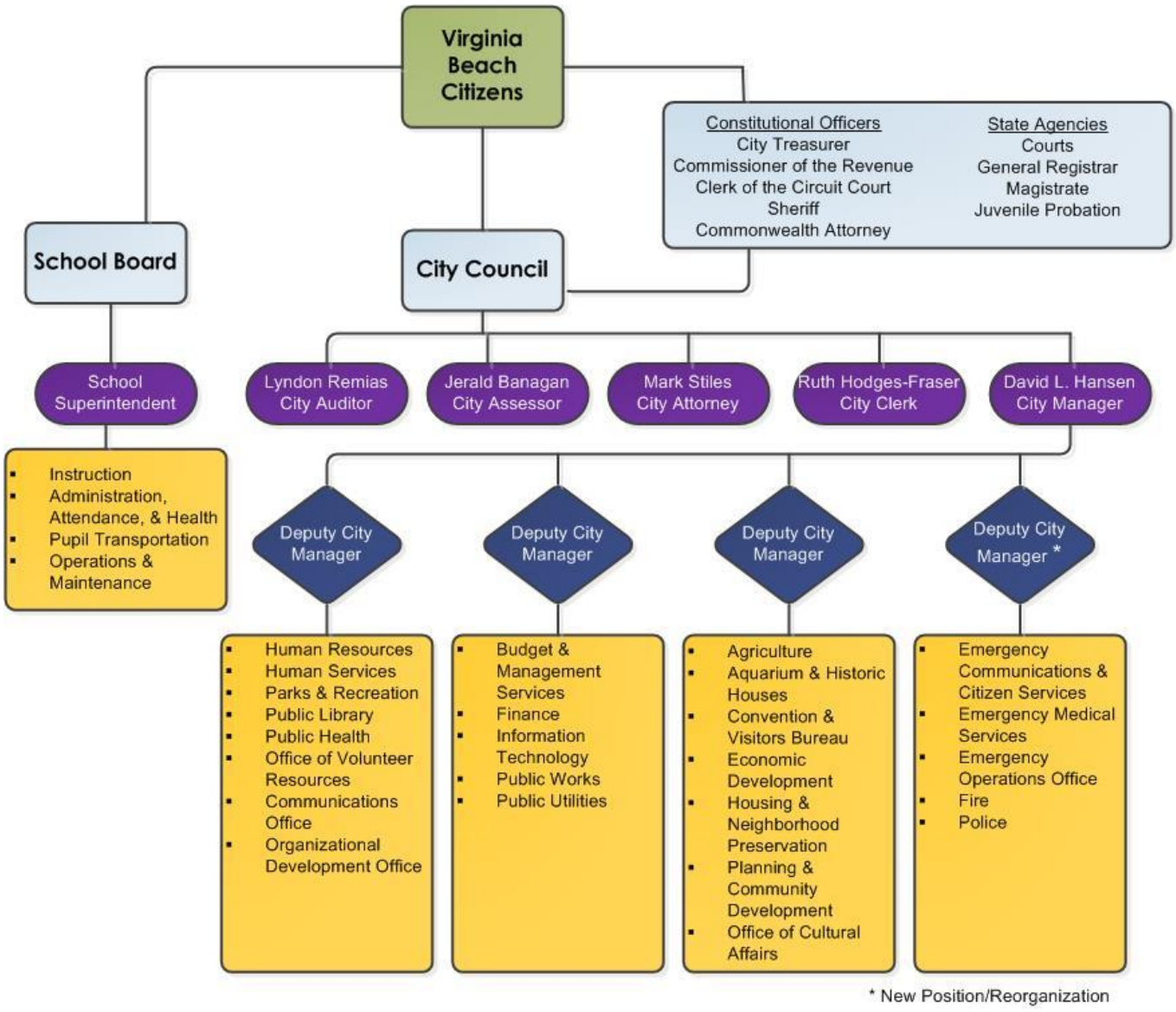
Negotiations shall then be conducted with each of the Offerors so selected. Price shall be considered, but need not be the sole determining factor. After negotiations have been conducted with each Offeror so selected, the City shall select the Offeror, which in its opinion, has made the best proposal, and shall award the contract to that Offeror. Should the City determine in its sole discretion that one Offeror is qualified, or that one Offeror is clearly more highly qualified than the others under consideration, a contract may be negotiated and awarded to that Offeror. The City of Virginia Beach is not required to furnish a statement of the reason(s) why a proposal was not deemed to be the most advantageous.

U. SUBMITTAL

The Offeror shall submit the following documents/information with their proposal:

1. Cover page of Request for Proposal with signature, title, and date;
2. Completed Anticollusion/Nondiscrimination/Drug-Free Workplace form (page 2);
3. Completed Subcontracting Participation Plan form (page 3);
4. Proposal as requested herein under Section VII, Subsection P, entitled "Preparation Guidelines";
5. Completed Attachment D Specification of Computing Environment Hardware and System Software;
6. Attachment E Database Questionnaire;
7. Attachment F ESInet Services and Software Investment Summary;
8. Attachment G Confidentiality Agreement;
9. Attachment H Requirements Compliance Summary Matrix

ATTACHMENT A – CITY OF VIRGINIA BEACH GOVERNMENT ORGANIZATIONAL STRUCTURE



ATTACHMENT B – CITY OF VIRGINIA BEACH COMPUTING ENVIRONMENT AND INFORMATION TECHNOLOGY STANDARDS

The City of Virginia Beach has a comprehensive computing environment that encompasses a broad array of computing platforms, as well as the complimentary systems software. This attachment provides information about the City's computing environment and associated standards and guidelines. It should be noted that not all documented environments apply to this RFP.

A. Network Environment

Network Hardware

Switched:	Switches are installed in a tiered architecture with strict access, distribution, edge and core components.
Routed:	The network is fully routed with Layer 3 boundaries between the core and all distribution points.
Wireless:	Wireless is provided in a manner that allows authenticated guest access, unauthenticated public users access and user/machine authentication for staff access. Wireless is provided inside and outside.
Standardization:	The City has elected Cisco as its standard for network hardware.

Security Hardware

Firewalls:	Firewalls are used at specific network boundaries in a measured manner that allows for granular control of access to City resources. Firewalls are configured to provide redundancy.
IDS/IPS:	Intrusion detection and prevention systems are placed throughout the network to promote better network threat visibility and mitigation.
Standardization:	The City uses a mixture of security platforms.

Network Software

Network Monitoring:	Network monitoring systems are used to track and benchmark service levels as well as to alert staff when action is necessary.
Network Management:	Management software is leveraged to provide scheduled jobs to run on network devices. This software also conducts routine backups of device configurations and applies updated software as necessary.
Network Access:	Access control software is employed to validate user provided credentials in order to gain access to network devices and areas of the network.

Topology

Campus:	A standard campus topology featuring hub-and-spoke design is used on campus.
Remote:	WAN sites are connected to the City's core through a variety of ISP provided technologies.
Connection Technologies:	ISP services include, as of the time of this writing, Metro-E, Cable, TLS, Point-to-Point, Frame-Relay, DSL and Wireless Cards.

Remote Access Security

Several types of vendor remote access are allowed:

Unmonitored access through VPN or Citrix:	Access is allowed into specific Development areas. Citrix access is used to log into a desktop computer and use an application. A VPN connection can be used for SQL access, access to Web applications and logging into specific computers. The vendor is not allowed to log into a server.
Monitored access through Citrix:	The vendor can be allowed access to any environment if access is monitored and managed by the City. This is a shadowed session.
WebEx, Live Meeting and GoToMeeting are also available.	

Modem access directly to systems located on the network is not authorized and will not be considered.

B. Server Environment

Server Configuration and Security

The City of Virginia Beach has standardized on Microsoft's Hyper-V virtualization platform for implementation of all supported workloads. Hyper-V servers are clustered at the host level to provide hardware fault tolerance. Guest operating systems supported in the City's virtual infrastructure are Windows Server 2003 Enterprise Edition, Windows Server 2008 Enterprise Edition and Windows Server 2008 R2 Enterprise Edition.

In situations where virtualization is not supported, HP BL460 Blade Servers or HP DL380s are utilized. Standard physical server configurations include dual, multi-cored processors, redundant power supplies, 32GB of RAM and mirrored hard drives for the operating system. The servers are housed in a secure, humidity and temperature controlled environment. Access to servers is controlled by physical and logon security to maintain the integrity of the machine.

Installation and configuration documentation is required prior to any installation. System installation and configuration must occur in the City test environment prior to use in production. Installation is performed by City personnel with assistance from the contractor if necessary. The City will not ship equipment to the vendor for software or hardware installation.

Web Server Hardware and Software

Windows Server 2008 Enterprise and Windows Server 2008 R2 Enterprise are the operating system platforms used for hosting Web sites on both the DMZ and Internal Networks. Web applications must support IIS 7.0. Internal Network Web Servers are member servers in the VB Active Directory domain. The DMZ Web Servers are stand-alone servers with no connection to Active Directory domain information hosted on the internal network. Microsoft file shares are not allowed to exist on servers residing on the DMZ. Remote Desktop sessions sourced from the internal network are permitted when required to support updates on servers located on the Internal Network. If a web component of software residing on a Web Server needs to exchange data with an Application Server then the Web component must support configurable socket communications. All servers utilize McAfee Antivirus Protection, which may not be disabled. Also, all servers participate in one of the City's Enterprise backup solutions, which includes off site tape storage.

Application Server Hardware and Software
Windows Server 2008 Enterprise and Windows Server 2008 R2 Enterprise are the operating system platforms used for hosting applications on the Internal Network. Application servers will be member servers in the VB Active Directory domain. Monitored access via Citrix will be allowed when required to support updates by maintenance personnel. Applications residing on Application servers will run as services, not applications. No user will be logged on during normal operations. All servers utilize McAfee Antivirus Protection, which may not be disabled. Also, all servers participate in one of the City's Enterprise backup solutions, which includes off site tape storage.

Database Server Hardware and Software
Windows Server 2008 Enterprise and Windows Server 2008 R2 Enterprise are the operating system platforms used for hosting databases on the Internal Network. Database servers are member servers in the VB Active Directory domain. Microsoft SQL 2005, SQL Server 2008 R2 database, and SQL Server 2012 database servers exist which are processor licensed to allow unlimited access where necessary. The City utilizes per CAL licensing for SQL servers where unlimited access is not required. These types of servers will be utilized for hosting database-related data required by new systems. When necessary, Oracle is also available. Monitored access via Citrix will be allowed when required to support updates by maintenance personnel. All servers utilize McAfee Antivirus Protection, which may not be disabled. Also, all servers participate in one of the City's Enterprise backup solutions, which includes off site tape storage.

Report Server Software
The City of Virginia Beach utilizes Microsoft SQL Server 2005 and Microsoft SQL Server 2008 R2 Reporting Services. Oracle Discover and Oracle Reports software are used for Oracle report development. The City strongly encourages that SSRS reports be configured for OleDB and be easily deployable to an enterprise consolidated infrastructure whether they are embedded in the solution or individual report objects.

Enterprise Storage System
The City of Virginia Beach uses a Storage Area Network (SAN) solution for centralized storage of data files such as documents, images, and raw data for Internal Web, Application, and Database servers and users. The iSCSI protocol is utilized to connect Database servers and Hyper-V hosts to the SAN.

Enterprise Backup Systems
The City of Virginia Beach uses two enterprise backup systems: Symantec NetBackup and Microsoft Data Protection Manager. Both systems store backups to tape or disk. Microsoft Data Protection Manager is used to protect systems on the internal network and NetBackup is used to protect all other systems. In addition, databases are backed up using the NetApp SnapManager solution and stored on a NetApp volume. Once a week the volume is backed up to tape for off-site storage.

C. Desktop Computer and Printing Environment
Desktop computers are retired and replaced departmentally on a cyclic basis, which is approximately every five (5) years. All desktop computers are provided connectivity through the City's LAN/WAN networked environment.

Desktop Computer Configuration
The City of Virginia Beach deploys HP Elite Computers (Mid Tower) with the following base specifications:

- 4GB of RAM

- 160GB SATA Hard Drive
- Sound capability
- 10/100 NIC (Network Interface Card)

The City of Virginia Beach also deploys HP Elite Book (laptop) with a 15.6" or 12.1" screen and the following base specifications:

- 4GB of RAM
- 160GB or 250 GB SATA Hard Drive
- Sound capability
- 10/100 NIC (Network Interface Card)

The supported operating systems are Windows XP and Windows 7. Standard Enterprise applications are:

- Microsoft Office 2010including Outlook
- Adobe Reader X
- Flash Player 10
- Auto Desk
- Map Guide Viewer 6.5
- Citrix XenApp
- Win DVD
- Primo PDF
- Java 5 with update 10, 6 with update 14
- Initiator 1.3.1.25
- Windows Live Photo Gallery

Client Application Software Installation

SCCM (Systems Center Configuration Manager) client software will be installed on all desktop computers in order to allow for Enterprise patching, application deployment, inventory, reporting, and management capabilities. McAfee Anti-Virus and Spy Ware software will also be installed on all systems and will not be disabled.

SCCM is used to fully automate the initial computer build and Enterprise application roll-out. The City performs this task in SCCM via OSD (Operating System Deployment), with MDT (Microsoft Deployment Toolkit) integration. Users are not authorized local administrative rights or privileges.

Printer Configuration

The connection standard for the City is a network-connected printer utilizing TCP/IP based printing, and spools through a network Print Server.

D. Mobile Data Computers

The City's Public Safety Departments use approximately 500 MDCs to access the City's Public Safety network and applications. The MDCs are ruggedized workstations running Windows 7 with 4GB RAM and 256GB solid state hard drives (SSD), and embedded GPS tracking. The mobile computers run on a Verizon 4G LTE embedded modem for network connectivity. All MDCs will be up-fitted with a ruggedized 802.11/n mobile router with AES encryption to facilitate a wireless hotspot around the vehicle. Some police units are also equipped with in-car DVM video recording devices that also utilize the MDC and mobile router. In the future, Advanced Authentication using smart card technology will be employed to access all police MDCs. EMS ambulances are additionally equipped with Panasonic Toughbooks and wirelessly connected tablets running the City's ePCR application in the back of the vehicles.

E. Hi-volume Printing

The City uses a Xerox DocuTech 128 HLC printer, which has highlight color capabilities for high-volume print jobs. Using Lytrod's Proform Designer software, forms can be designed to merge with data from applications. The preferred file format for the data to be merged with forms is an ascii data file that is comma or tab delimited (Excel). Other standard Windows print files can also be printed (Word, PDF). In Printing Services, the City uses a Xerox DocuTech 6135 printer for high-volume black only print jobs and a DocuColor 260 for full color capabilities. Both use Xerox Free Flow software. The preferred file format for printing is PDF and Windows applications print files.

F. Development and Test Environment

The City conducts security, functional and user testing to verify the application works securely and properly in the VB network environment. Once the system has been tested and approved to be moved to production, City personnel, with Vendor assistance if necessary, install the system into production. The test environment installation remains operational concurrent with the production system for subsequent change and problem evaluation. All changes, upgrades or problem evaluation will be performed first on the test system.

G. GIS Environment

GIS uses the City standard desktop computers described in section C-1 of this document.

Software Solution Standards

- Spatial information will reside in either Oracle RDBMS or MS SQL Server RDBMS
- Spatial geometry will be stored as SDO_Geometry or ST_Geometry.
- GIS systems, designs and formats must read and write directly to either Oracle SDO_Geometry (in Oracle) or ST_Geometry (in either RDBMS environment) formats.
- The RDBMS minimum version compatibility requirement is either Oracle 11.G R2 or SQL Server 2012 for the current GIS databases.
- The Urban and Regional Information Systems Association (URISA) model is the GIS Geocoding standard.
- National Emergency Management Association (NEMA/URISA) is the addressing standard. Please reference http://www.urisa.org/about/initiatives/addressstandard
- For the streaming GPS the City must use the National Marine Electronics Association (NMEA) 0183 standard. The GPS reads the text based log file to post the users current location. Please reference http://www.nmea.org/
- For the posting locations we prefer using the USNG United States National Grid. Please reference http://www.fgdc.gov/usng.

Spatial Data Collection Project Standards

- Spatial data must be delivered in current datum:
  - Horizontal: (NAD 83/93 (HARN), Virginia State Plane Coordinate System, South Zone, Lambert conformal (Conic), US Survey Foot), at the specified accuracy
  - Vertical: NAVD 88, at the specified accuracy
- Spatial data to be imported into the GIS system must be delivered in one of the following formats:
  - Oracle database export in either SDO_Geometry or ST_Geometry
  - MS SQL Server Export in ST_Geometry
  - Intergraph data formats (Oracle Object Model (OOM), Geomedia Feature Class)
  - ESRI feature classes inFile or Personal Geodatabase v 9.3.1
- Tabular data to be imported into the GIS system must be delivered in one of the following formats:
  - Oracle

- MS SQL
- ASCII or other text format (Comma delimited)
- LIDAR
- GeoTIFF
- GeoJPG
- MrSID
-

H. Voice Systems

The City's current PBX configuration for the Municipal Center is Avaya CS1K. Any application that interfaces with voice mail systems must be compatible with Avaya Call Pilot, which is the City's Voice Mail System. The City utilizes Nortel's Contact Center ACD system and Nortel MPS 500 IVR system. Any required interfaces with these types of systems must be compatible. The City has its own NXX of 385-0000 to 385-9999 block of telephone numbers for all systems attached and running off of the Municipal Center PBX and uses 4-digit dialing. The City's future systems will include Microsoft Voice VoIP and Cisco Voice VoIP platforms. Solutions that integrate with these future systems are preferred. The use of Session Initiation Protocol (SIP) will be heavily leveraged to provide effective control of communications sessions. This control includes call setup, modification and teardown.

I. Radio Systems

The City's current radio system is a Motorola Astro P25 Digital Radio Simulcast System.

J. Audio Visual (Multimedia) Environment

All audio-visual proposed solutions must meet the National Fire Protection Association's (NFPA) National Electric Code (NEC) standards. The City standards for CAD drawings of the proposed multi-media solution are the AutoCAD formats dwg or dxf. Still cameras with the ability to save in raw format (uncompressed or lossless) are encouraged. The City standard for still photo editing and archiving is software that is able to work with the following formats:

- Raw
- Jpeg
- Photoshop document (psd)
- Digital negative (dng)

K. City Web Sites

Web sites must be compliant with both the American Disability Act (ADA) and with the Worldwide Web Consortium (W3C). The City is moving toward an Enterprise SharePoint solution for content management for internal and external web sites. SharePoint plug-ins and web parts are strongly encouraged. The City supports the use of alternate technologies such as XML, web services and COM+. City web pages are compatible with Microsoft Internet Explorer Version 7.0 and higher, Firefox, Safari and Google Chrome. They are viewable at 1024X768 resolution with dynamically resizable windows. Secure web pages use the secure socket layer (SSL) with 128 bit encryption.

L. Collaboration

Microsoft SharePoint Enterprise is a key enterprise strategy for the sharing and distribution of information. Departments are progressively managing more of their information and records using SharePoint. Solutions that leverage these capabilities are preferred.

M. Application Software

New applications are encouraged to be Active Directory (AD) aware to take advantage of the Enterprise security afforded by AD. Local application security databases that store passwords are

strongly discouraged. Web-based applications based on or built around Microsoft technologies are preferred over Client Server architecture. The applications should be flexible and customizable to integrate with city-developed web sites where applicable.

Standards include:

- SQL Server 2008 or higher
- Windows Server 2008 Enterprise and Windows Server 2008 R2 Enterprise with IIS 7.0
- For internal applications, Internet Explorer 7 or higher
- For public facing applications, cross-browser compatibility (Internet Explorer 7 or higher, Firefox, Safari and Google Chrome)
- Where applicable, latest version of SSL with 128-bit encryption
- Viewable at 800X600 resolution
- XML and Web services for Application interfaces (APIs)
- Hooks where necessary for XML and web services
- SQL Server Integration Services (SSIS) for developing batch processes
- If the application requires Java Runtime, then it must meet the standards for desktop applications above
- If the COTS supports a reporting component, SQL Server Reporting Services are used

Preferences include:

- Application framework .NET 2.0
- Web services architecture
- Pages in which the page controls adjust automatically as the window size is changed
- Use of applets, plug-ins or active-x is discouraged

N. Project Management Standards

Project processes are aligned with the Project Management Institute's standards as defined in the Guide to the Project Management Body of Knowledge (PMBOK® Guide). Projects are managed by a City project manager in cooperation with a project manager for the Contractor. The project management information system is Microsoft Project Server. Project schedules are maintained in Microsoft Project. Changes to the plan are controlled through a formal change management process. For new system implementations and major upgrades, the standard project process includes:

- Joint project planning sessions with City and Contractor project team members
- Approval of the project plan by all stakeholders
- Requirements gathering and approval by functional and technical stakeholders
- Fit analysis to identify and resolve gaps in functionality
- System design and approval by the City's Design Review Board
- Establishment of a test environment
- Training of functional and technical leads
- Revision of business processes
- Development of test plans and scenarios
- Adoption of system acceptance process
- Conversion testing
- Product acceptance testing
- Adoption of production implementation plan
- Training of end users
- Go-live in production environment
- Post-production support

O. Standard Enterprise Application Software

The City uses the following enterprise solutions:

- McAfee Virus Scanning
- Citrix
- Oracle Government Financials 11i
- Exchange 2010
- MS Explorer 6/7/8.x Web Browser
- MS Project Server (Thick and Thin)
- What's Up Gold V11
- Heat
- LaserFiche Imaging (with Web Component)
- COTS from Hansen, OSSI (Pistol), Red Alert, Tiburon, and many, many others
- HP - Quality Center, Load Runner
- SharePoint

P. Destruction of Sensitive Data

Acceptable means to destroy rigid magnetic media such as floppy disks, hard drives, CD-ROM, DVD-ROMs, and tapes are described below:

- Destruction by bulk degaussing. Tapes, diskettes, hard drives, and other electronic storage media can be rendered inert by a degausser. Degaussing removes the magnetic properties of the material and makes the media un-useable for future use. Degaussing should only be performed by individuals who are familiar with the degaussing equipment.
- Physical destruction/impairment beyond reasonable use. Floppy disks can be cut into strips by using scissors. The floppy disk should be removed from the covering, cut into several strips and cross-cut at least twice. Floppy disks can also be shredded in a crosscut shredder. Again, remove the disk from the covering and feed the disk into the shredder.
- Optical mass storage media, including compact disks must be destroyed by burning, pulverizing, or grinding the information-bearing surface. Burning shall be performed only in a facility certified for the destruction of materials. Plastic CDs and DVDs can be destroyed by breaking them in small pieces.

Q. Service Standards

The Support Center is the City's central point of contact for receiving and managing requests for service, change management, and for providing customer notification regarding service.

Incident Management Process

The City Support Center currently uses SolarWinds Web Help Desk (WHD) software incident management system to record and track service requests.

The City has defined four priority classifications of service and expected response times:

Priority 1 Service requests are defined as unplanned system outages that affect multiple employees Citywide or, an entire department and prohibit production processing. The response target is to acknowledge priority one calls within 15 minutes and resolved them within 2 hours.

Priority 2 Service requests are defined as a small-scale system outage that affects a number of employees but, not an entire department or the enterprise. The response target is to acknowledge priority two calls within 30 minutes and resolved them within 9 hours.

Priority 3 Service requests are defined as a service outage or a functional problem that affects one employee. The response target is to acknowledge priority three calls within 3 hours and resolved them within 27 hours.

Priority 4 Service requests are defined as scheduled work that needs to be performed. The response target is to acknowledge priority four calls within 9 hours and resolved them within 8 days. Examples of priority 4 requests are new customer accounts and scheduled software installations.

Change Management Process

All changes to production systems and equipment that require a service outage or, can reasonably be expected to have adverse impact on customer services are managed by the change management process. A formal change request must be submitted to the Support Center for all changes, both scheduled and unscheduled, and are tracked in the incident management system. Changes are approved and scheduled during the weekly Change Management Review meeting and customers are notified of all changes in advance.

R. Externally Hosted Solutions

Infrastructure

- A hosting facility with dual power supplies with commercial power and separate uninterrupted power supplies. The Uninterrupted Power Supply (UPS) facility must be composed of battery back-up services sufficient to support power transition to the secondary power provided by diesel generators.
- Hardware platform, operating system, system application and database maintenance.
- Secure infrastructure where the servers and other hardware are physically inaccessible to unauthorized users
- Security technologies including data encryption, user authentication, perimeter defense, operating system safeguards, and storm- and attack-hardened datacenters
- Redundant communication infrastructure
- Data and System recovery capabilities, including disk mirror imaging and daily backup of data with off-site storage cycled on a daily basis
- Back-up facility/infrastructure to support a disaster recovery plan
- Backups of data and software with off-site storage to support a disaster recovery plan
- Off-site storage in an environmentally controlled and secure location

Services

- Access to the application for an agreed upon number of active or named users as applicable
- Access to the database for an agreed upon number of report and interface developers
- Contractor-signed Confidentiality agreements for sensitive data
- Compliance with Destruction of Sensitive Data standards above
- Security audits
- Reporting of application access and utilization statistics, such as Web analytics
- Operations control, maintenance and monitoring of the application during agreed upon hours including problem identification and resolution, escalation and notification
- Compliance with Service standards above
- Disaster recovery planning
- System administration including system backup and recovery, performance tuning and capacity planning, configuration management, and data backups and restores
- Database administration including

- Hardware and software review (memory, disk volumes, operating system levels and any additional software required)
- Compatibility review with existing software
- RDBMS installation
- Recovery documentation
- Upgrades and patch support
- Database backup software resolution
- Automatic notification of events
- Automatic action on selected events (software failures)
- Security reporting
- Capacity planning
- Disk utilization reporting

Attachment B – Name (please print):_____

Title: _____

Contractor Name: _____

Signature: _____

Date: _____

ATTACHMENT C - CITY OF VIRGINIA BEACH PSAPS WITH LIST OF PREFERRED INTEROPERABLE AGENCIES

I. City of Virginia Beach Primary PSAPs

The City of Virginia Beach has two locations for the City of Virginia Beach ESInet. The primary location is the Emergency Communication Center which is the PSAP for the City of Virginia Beach. It is located at 2508 Princess Anne Rd, Virginia Beach, VA 23456. The City has a designated back-up PSAP which is located at 4160 Virginia Beach Blvd, VA 23462.

II. Other Public Safety Entities in City of Virginia Beach Jurisdiction

The following agencies have public safety responsibilities for emergency calls originating from their locations inside the City of Virginia Beach. Calls are currently transferred over the Public Switched Network, however the City is interested in possibly including these agencies as trusted entities on the City of Virginia Beach ESInet.

- Dam Neck Naval Base
- Oceana Master Jet Naval Base
- Joint Expeditionary Base Little Creek/Fort Story
- Regent University
- Norfolk International Airport

III. Legacy PSAPs on Regional Verizon Mated Selective Routers Interoperability Agencies

The City of Virginia Beach currently has the ability to do PSAP to PSAP transfers, delivering voice and ANI, to neighboring PSAP jurisdiction that utilize the same Verizon mated Selective Routers. Some of these neighboring agencies may opt to participate in the City of Virginia Beach. However, unless or until they do the following agencies must be able to interoperate with the City of Virginia Beach ESInet via the Legacy Gateway Interoperability requirements set for in the Technical Requirements of this RFP:

Chesapeake *	James City *	Suffolk *
Eastern Shore *	Newport News *	Surry *
Franklin City *	Norfolk *	Virginia Beach *
Hampton *	Portsmouth *	York-Poquoson-Williamsburg *
Isle of Wight *	Southampton *	

IV. ESInet Interoperability Agencies

PSAPs in the Commonwealth of Virginia are actively pursuing deployment of ESInet services. It is likely other areas of Virginia as well as jurisdictions in North Carolina which are adjacent to the City of Virginia Beach will have different ESInet providers. Therefore the list of jurisdiction below which do not work on the same Selective Routers currently serving the City of Virginia Beach should be considered as preferred interoperability agencies. The Technical Requirements for ESInet Interoperability shall be applicable for these agencies:

Alexandria
Alleghany
Amelia
Amherst
Appomattox
Arlington
Augusta
Bath
Bedford
Bland
Botetourt
Bristol
Brunswick
Buchanan
Buckingham
Campbell
Caroline
Charles City
Charlotte
Charlottesville-UVA-Albemarle
Chesterfield
Clarke
Colonial Heights
Covington
Craig
Culpeper
Cumberland
Currituck County, NC
Danville
Dickenson
Dinwiddie
Emporia
Essex
Fairfax
Falls Church
Farmville

Fauquier
Floyd
Fluvanna
Franklin County
Frederick
Fredericksburg
Giles
Gloucester
Goochland
Greene
Greensville
Halifax
Hanover
Harrisonburg-Rockingham
Henrico
Highland
Hopewell
King and Queen
King George
King William
Lancaster
Lee
Loudoun
Louisa
Lunenburg
Lynchburg
Madison
Manassas
Manassas Park
Martinsville-Henry
Mathews
Mecklenburg
Middlesex
Nelson
New Kent
New River Valley
Northumberland

Norton
Nottoway
Orange
Page
Patrick
Petersburg
Pittsylvania
Powhatan
Prince George
Prince William
Pulaski
Radford
Rappahannock
Richmond Ambulance Authority
Richmond City
Richmond County
Roanoke City
Roanoke County
Rockbridge
Russell
Salem
Scott
Shenandoah
Smyth
Spotsylvania
Stafford
Staunton
Sussex
Tazewell
Twin County
Warren
Washington
Waynesboro
Westmoreland
Winchester
Wise
Wythe

ATTACHMENT D - SPECIFICATION OF ENVIRONMENT HARDWARE AND SYSTEM SOFTWARE

Listed below are instructions for providing system hardware and system software specifications to support the proposed solution. The Offeror is fully responsible for providing the City with a complete configuration specification.

A. Server Hardware

List the number and type of servers (web, app, database, report, batch, etc.) recommended. For each server, provide the following information:

1. Central Processor, Memory, Storage, and Network Connection Speed -
   Specify the server's central processor(s), random access memory, configuration, disk capacity and network connection speed required to connect the server to the City's network.

   Note: The system must allow for linear growth within the same family of hardware without replacement.

2. Other
   Specify any other required hardware component.

B. Server Software

For each required server, provide specifications for a comprehensive server software environment. Please include version, release level and licensing details in the specifications. The specifications may include as applicable:

1. Operating System Software
2. Application Services Components
3. Application Development Tools
4. Performance Tools
5. Education Tools
6. System Management Tools
7. System Security Tools
8. Utility Tools
9. Job Scheduling Tools
10. Report Execution, Distribution, or Archive Tools
11. Backup Management/System Tools
12. Disk Management Tools
13. Database Management System Software
    If non MS SQL Server is used as the database backend, also specify the client access licensing required for the proposed system.
14. Query/Report Writing Software
15. Software Required to Connect Server to City Network
16. Other

C. Other

Specify any other hardware not identified in the previous section that will be included with the proposed solution.

ATTACHMENT E – DATABASE QUESTIONNAIRE

Note: This section to be completed by Offeror's if they intend to install ESInet applications and/or servers within the City's technology environment. If not, please state "Attachment E – Not Applicable" in Bid Response.

General Product Information

#	Item	Values	Notes
1	Product name		
2	Version number		
3	Contractor website		
4	Minimum database server hardware requirements documentation included	☐ Yes ☐ No	
5	Database installation documentation included	☐ Yes ☐ No	
6	Software compatibility matrix included	☐ Yes ☐ No	

Database information

#	Item	Values	Notes
7	RDBMS and version number	☐ Oracle ☐ SQL Server ☐ Other	
8	Database edition	☐ Enterprise ☐ Standard ☐ BI ☐ Express ☐ Other	
9	Database license type	☐ Per user ☐ Per processor ☐ Other	
10	RDBMS current service pack		
11	Operating system name and version	☐ UNIX ☐ MS Windows Enterprise ☐ MS Windows Standard ☐ Linux ☐ Other	
12	Operating system current service pack		

#	Item	Values	Notes
13	Application type	☐ OLTP ☐ Reporting ☐ OLTP and Reporting ☐ Batch processing	
14	Application use	☐ Infrastructure support ☐ Line of business	
15	Number of databases to support application	☐ One ☐ Two or more on the same server ☐ Two or more on different servers ☐ Other	
16	Initial database load and size	☐ Start from empty database ☐ Requires initial load ☐ Requires data conversion from other systems	
17	Database installation procedure	☐ Contractor provided scripts ☐ Executable ☐ Manual ☐ Other	
18	Rate of data growth	☐ Per year ☐ Per month	
19	Data archiving /purging tools/scripts provided	☐ Yes ☐ No ☐ Can be custom developed	
20	DBA maintenance plan included	☐ Yes ☐ No ☐ Have to be developed by customer	
21	Enhanced Server features and database features used	☐ Spatial ☐ Partitioning of data and indexes ☐ Replication ☐ Analysis services ☐ SQL Email ☐ FTP ☐ Other	
22	Application requires the reporting module	☐ Crystal reports ☐ Reporting Services ☐ Canned reports included ☐ Extensions allowed to the existing reports ☐ Other reporting features – please specify	

#	Item	Values	Notes
23	If reporting module is provided please specify additional requirements needed in	☐ Software installation ☐ Hardware ☐ Licensing	
24	Third party applications to be installed on the database server	☐ Yes ☐ No	
25	How many database environments is needed to support application	☐ Production ☐ Development ☐ Test ☐ Training ☐ Other	
26	Does database support being run in the consolidated environment	☐ Yes ☐ No	
27	Database recovery mode	☐ Full ☐ Simple	
28	Database extensions/ enhancements allowed in the database (adding new objects like indexes)	☐ Yes ☐ No	
29	Database auditing requirements	☐ Yes ☐ No ☐ Not applicable	
30	HIPPA compliance requirements	☐ Yes ☐ No ☐ Not applicable	
31	Data encryption requirements	☐ Yes ☐ No ☐ Not applicable	
34	High availability support	☐ Cluster ☐ SQL AlwaysOn High Availability ☐ DR/Multi-Subnet support	
35	Maximum number of users of the application		
36	Database upgrade plan is part of support model	☐ Yes ☐ No	
37	Database security module	☐ AD compliant ☐ Application driven ☐ Database driven	
38	Procedure for database cloning/copying included	☐ Yes ☐ No ☐ Not applicable	
39	Application allows ad hoc queries and what method is used		

#	Item	Values	Notes
40	Custom interfaces with other data sources included	☐ Yes ☐ No ☐ Not applicable	
41	Connection user password requirements		
42	Database users and roles provided	☐ Yes ☐ No	
43	Exception and error handling is provided and is recorded in the:	☐ Event log ☐ Application log ☐ Database log	
44	User error notification included – please specify method		
46	Customized database and server configuration is handled by	☐ Application GUI ☐ Database direct table update ☐ Other ☐ Not allowed	
47	File I/O permissions needed – please specify	☐ Yes ☐ No	
48	If the applications produces output files they are stored on	☐ A network ☐ In a database	

ATTACHMENT F – ESINET SERVICES AND SOFTWARE INVESTMENT SUMMARY

City of Virginia Beach RFP #_ITAS-19-0065_____

ESInet NON-RECURRING COST INVESTMENT SUMMARY

Offeror Name _____

Project	Cost
Application Software Licenses	
Enterprise License	_____
Server license	(+) _____
(If the system is a modular system – Break out the costs of each module in accordance to number of licenses for a ___-___ user system)	
User license for ___-___ users	(+) _____
Licensing for ___-___ workstations	(+) _____
Other Licenses required (specify)	(+) _____
Total Application Software Licenses	_____
Third Party Application Software Licenses (specify, insert lines)	
_____	_____
_____	(+) _____
Total Third Party Application Software Licenses	_____
Total Cost of Modifications	
List the total cost for all identified modifications to proposed software solution	_____
Hardware (specify, insert lines)	
_____	_____
_____	(+) _____
_____	(+) _____
Total Hardware	_____
Specialized ESInet Support (specify products)	
	_____
	(+) _____
Networking	(+) _____
DBMS	(+) _____
Report Writer Software	(+) _____
Other Specialized Services	(+) _____
Total Cost of Specialized ESInet Support	_____

Project	Cost
Implementation Services	
Project Management	_____
Business Analysis	(+) _____
Data Conversion/Migration	(+) _____
Training (specify, insert lines)	
End-user training	(+) _____
_____	(+) _____
Other Services (specify, insert lines)	
_____	(+) _____
Total Cost of Implementation Services	_____
Travel Expenses	_____
Other (specify, insert lines)	
_____	_____
_____	(+) _____
Total Cost of other products, services or expenses	_____
Total Project Non-Recurring Cost	_____

ESInet RECURRING COST INVESTMENT SUMMARY

Maintenance and Support Ongoing Costs	Cost
Annual Application Software Maintenance Fees (to include all updates and releases)	_____
Annual Hardware and System Software Support Costs	_____
Annual Network Recurring Costs	_____
Annual Database and GIS Recurring Costs	_____
Other Ongoing Costs (specify)	_____
_____	(+) _____
_____	(+) _____
Total Ongoing Cost	_____

Ten Year Ongoing Cost	Cost
Year 1	_____
Year 2	(+) _____
Year 3	(+) _____
Year 4	(+) _____
Year 5	(+) _____
Year 6	(+) _____
Year 6	(+) _____
Year 8	(+) _____
Year 9	(+) _____
Year 10	(+) _____
Total Ten Year Ongoing Cost	_____

Name (please print):_____

Title: _____

Contractor Name: _____

Signature: _____

Date: _____

ATTACHMENT G – CONFIDENTIALITY AGREEMENT

City of Virginia Beach
Department of Information Technology
Authorized Workforce Confidentiality Agreement
For Work Related to RFP #ITAS-19-0065

This Agreement between the City of Virginia Beach, and_____, on temporary assignment for work specifically related to RFP #_ITAS-19-0065, hereby acknowledges that many records being retained by the City or handled by staff are considered privacy protected and are not to be disclosed to any unauthorized individual, company, or government agency.

I acknowledge that there are both state and federal laws that limit who can access certain records. These laws include penalties for breaches of confidentiality.

Unauthorized use, dissemination or distribution of confidential records including but not limited to protected health information, police records, information that identifies persons receiving federal aid, and any City data not normally available to public scrutiny, may constitute a crime.

I hereby agree that I will not use, disseminate or otherwise distribute confidential records or information either on paper or by electronic means other than in the performance of the specific job roles I am authorized to perform. No request will be honored without specific written authorization from the custodian of the record or through direct written communication with the Contract Administrator or the Office of the City Attorney.

I also understand that unauthorized use, dissemination or distribution of confidential information may result in both civil and criminal penalties.

Name (please print):_____

Title: _____

Contractor Name: _____

Signature: _____

Date: _____

ATTACHMENT H: REQUIREMENTS COMPLIANCE SUMMARY MATRIX

Requirement	Understood	Complies	Complies Partially	Complies with Future Capability	Does Not Comply	Response Provided
Section III, A,1 a,1						
Section III, A,1 a,2						
Section III, A,1 a,3						
Section III, A,2						
Section III, A,3						
Section III, A,4						
Section III, B,1,1						
Section III, B,1,2						
Section III, B,2						
Section III, B,3,1						
Section III, B,3,2						
Section III, B,3,3						
Section III, B,3,4						
Section III, B,3,5						
Section III, B,3,6						
Section III, B,3,7						
Section III, B,3,8						
Section III, B,3,9						
Section III, B,3,10						
Section III, B,3,11						
Section III, B,3,12						
Section III, B,3,13						
Section III, B,4,1						
Section III, B,4,2						
Section III, B,4,3						
Section III, B,5						
Section III, B,6,1						
Section III, B,7						
Section III, B,7, a,1						
Section III, B,7, a,2						
Section III, B,7,b						
Section III, B,7, c, 1						
Section III, B,7, c, 2						
Section III, B,7, d,1						
Section III, B,8,1						
Section III, B,8,2						
Section III, B,8,3						
Section III, B,8,4						
Section III, B,8,5						
Section III, B,8,6						
Section III, B,8, a,1						
Section III, B,8, a,2						
Section III, B,9,1						
Section III, B,9,2						
Section III, B,9,2,						
Section III, B,9,2,						
Section III, B,9,2,						
Section III, B,9,2,						

Requirement	Understood	Complies	Complies Partially	Complies with Future Capability	Does Not Comply	Response Provided
Section III, B,9,2, b						
Section III, B,9,2,						
Section III, B,9,2,						
Section III, B,9,2,						
Section III, B,9,2,						
Section III, B,9,2,						
Section III, B,9,2,						
Section III, B,9,2,						
Section III, B,9,2,						
Section III, B,9,2,						
Section III, B,9,2, g						
Section III, B,9,2, h						
Section III, B,9,2, i						
Section III, B,9,2, j						
Section III, B,9,2, k						
Section III, B,9,2, l						
Section III, B,9,2, m						
Section III, B,9,2,						
Section III, B,9,2,						
Section III, B,9,2,						
Section III, B,10						
Section III, B,10, a,1						
Section III, B,10, a,2						
Section III, B,10, a,3						
Section III, B,10, a,4						
Section III, B,10, a,5						
Section III, B,10, a,6						
Section III, B,10, a,7						
Section III, B,10, a,8						
Section III, B,10, a,9						
Section III, B,10,						
Section III, B,10,						
Section III, B,10,						
Section III, B,10,						
Section III, B,10,						
Section III, B,10, c,1						
Section III, B,10, c,2						
Section III, B,10, c,3						
Section III, B,10, c,4						
Section III, B,10, c,5						
Section III, B,10, c,6						

Requirement	Understood	Complies	Complies Partially	Complies with Future Capability	Does Not Comply	Response Provided
Section III, B,10,						
Section III, B,10,						
Section III, B,10,						
Section III, B,10,						
Section III, B,10,						
Section III, B,10,						
Section III, B,10,						
Section III, B,10,						
Section III, B,10,						
Section III, B,10,						
Section III, B,10,						
Section III, B,10,						
Section III, B,10,						
Section III, B,10,						
Section III, B,10,						
Section III, B,10, e,1						
Section III, B,10, e,2						
Section III, B,10, e,3						
Section III, B,10, e,4						
Section III, B,10, e,5						
Section III, B,10, e,6						
Section III, B,10, e,7						
Section III, B,10, e,8						
Section III, B,10, f,1						
Section III, B,10, f,2						
Section III, B,10, f,3						
Section III, B,10, f,4						
Section III, B,10, f,5						
Section III, B,10, f,6						
Section III, B,10, f,7						
Section III, B,10, f,8						
Section III, B,10, f,9						
Section III, B,10,						
Section III, B,10,						
Section III, B,10,						

Requirement	Understood	Complies	Complies Partially	Complies with Future Capability	Does Not Comply	Response Provided
Section III, B,10, g,1						
Section III, B,10, g,2						
Section III, B,10, g,3						
Section III, B,10, g,4						
Section III, B,10, g,5						
Section III, B,10, h,1						
Section III, B,10, h,2						
Section III, B,10, h,3						
Section III, B,10, h,4						
Section III, B,10, i,1						
Section III, B,10, i,2						
Section III, B,10, j						
Section III, B,10, k,1						
Section III, B,10, k,2						
Section III, B,10, k,3						
Section III, B,10, k,4						
Section III, B,10, k,5						
Section III, B,10, k,6						
Section III, B,10, k,7						
Section III, B,10, l,1						
Section III, B,10, l,2						
Section III, B,10, m,1						
Section III, B,10, m,2						
Section III, B,10, n						
Section III, B,11, a						
Section III, B,11, b,1						
Section III, B,11, b,2						
Section III, B,11, b,3						
Section III, B,11, b,4						
Section III, B,11, b,5						
Section III, B,11, b,6						
Section III, B,11, b,7						

Requirement	Understood	Complies	Complies Partially	Complies with Future Capability	Does Not Comply	Response Provided
Section III, B,11, b,8						
Section III, B,11, b,9						
Section III, B,11, b,10						
Section III, B,11, c						
Section III, B,11, d,1						
Section III, B,11, d,2						
Section III, B,11, d,3						
Section III, B,11, d,4						
Section III, B,11, e						
Section III, B,11, f						
Section III, B,11, g						
Section III, B,12,1						
Section III, B,12,2						
Section III, C,1						
Section III, C,2						
Section III, C,3						
Section III, C,4						
Section III, D,1						
Section III, D,2						
Section III, D,3						
Section III, D,4						
Section III, D,5						
Section III, E,1						
Section III, E,2						
Section III, F						
Section III, G,1,1						
Section III, G,1,2						
Section III, G,2,1						
Section III, G,2,2						
Section III, G,2,3						
Section III, G,2,4						
Section III, H						

References

DoD Documents

CJCSM 3150.03D, *Joint Reporting Structure Event and Incident Reports*
Deputy Secretary of Defense memorandum, *DoD Information Resources Management Strategic Plan*, April 1, 2015
DoDI 6055.06, *DoD Fire and Emergency Services Program*, Change 1, August 31, 2018
DoDI 6055.17. *DoD Emergency Management Program*, February 13, 2017
DoDI 8130.01, *Installation Geospatial Information and Services*
DoDI 8320.07. *Implementing the Sharing of Data, Information, and Information Technology Services in the Department of Defense*, Change 1, December 5, 2017
DoDI 8330.01, *Interoperability of Information Technology, Including National Security Systems*, Change 1, December 18, 2017
DoDI 8500.01, *Cybersecurity*
DoDI 8540.01, *Cross Domain Policy*, Change 1, August 28, 2017
DoD Strategic Management Plan, July 2013
Protecting the Force, Lessons from Fort Hood, Report of the DoD Independent Review, January 2010
Secretary of Defense Memorandum, *Final Recommendations of the Ft. Hood Follow-on Review*, August 18, 2010
USNORTHCOM Instruction 10-222, *Force Protection Mission and Antiterrorism Program*

Army Documents

AR 25-400-2, *Army Records Information System*
AR 70-1, *Army Acquisition Policy*
AR 190-45, *Law Enforcement Reporting*
AR 420-1, *Army Facilities Management*
AR 525-2, *The Army Protection Program*
AR 525-27, *Army Emergency Management Program*
Army Network Campaign Plan, ver. 1.1, February 2015
Computer Aided Dispatch Capability Problem Statement, June 18, 2015

Other

FCC Task Force on Optimal PSAP Architecture, *Adopted Final Report*, January 29, 2016
FCC TFOPA, Working Group 2: Optimal Approach to NG91-1-1 Implementation, Final Supplemental Report, December 2, 2016
National 911 Program, *Next Generation 911 Interstate Playbook*, June 2018
NENA/APCO Next Generation 9-1-1 Public Safety Answering Point Requirements, 04/05/2018

Acronyms and Abbreviations

ALI	Automatic location identification
AMC	Army Medical Command
ANCP	*Army Network Campaign Plan*
AoA	Analysis of Alternatives
AOR	Area of Responsibility
APL	Approved Products List
ASA (ALT)	Assistant Secretary of the Army (Acquisition, Logistics and Technology)
BCA	Business Case Analysis
CAD	Computer-Aided Dispatch
CCB	Configuration Control Board
CHE	Call Handling Equipment
CIO	Chief Information Officer
CLS	Common Levels of Service
CON	Certificate of Networthiness
CONUS	Continental United States
COP	Common Operating Picture
COOP	Continuity of Operations
DA	Department of Army
DoD	Department of Defense
DOTMLPF-P	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy
E911	Enhanced 911
EMS	Emergency Medical Services
EOC	Emergency Operations Center
ESInet	Emergency Services IP Network
ESN	Emergency Service Number
ESRP	Emergency Services Routing Proxy
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FOUO	For Official Use Only
GIS	Geographic Information System
HLO	High-Level Outcome

HQDA	Headquarters, Department of the Army
IA	Information Assurance
ICT	Information and Communications Technology
ILEC	Incumbent Local Exchange Carrier
IMCOM	Installations Management Command
IP	Internet Protocol
IRM	Information Resources Management
JITC	Joint Interoperability Test Command
LE	Law Enforcement
LMR	Land Mobile Radio
MDC	Mobile Data Computer
MDT	Mobile Data Terminal
MEDCOM	Medical Command
MOU	Memorandum of Understanding
MSAG	Master Street Address Guide
NCIC	National Crime Information Center
NENA	National Emergency Number Association
NG911	Next Generation 9-1-1
NGCS	Next Generation Core Services
POI	Program of Instruction
PMO	Provost Marshal Office
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
RMF	Risk Management Framework
SIP	Session Initiation Protocol
TDD/TTY	Telecommunications Devices for the Deaf/Teletypewriter
TDM	Time Division Multiplexing
TFOPA	Task Force on Optimal PSAP Architecture
TIGER	Topologically Integrated Geographic Encoding and Referencing
TRADOC	Training and Doctrine Command
TSP	Training and Support Package
VoIP	Voice over IP

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
00-05-19	Final	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Department of the Army: Closing the Next Generation 9-1-1 Capability Gap	HQ0034-14-D-0001
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)	5d. PROJECT NUMBER
Serena Chan, Michael T. Hernon	BC-5-4012
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES	8. PERFORMING ORGANIZATION REPORT NUMBER
Institute for Defense Analyses 4850 Mark Center Drive Alexandria, VA 22311-1882	D-10648

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR'S / MONITOR'S ACRONYM
Katherine Brennan HQDA OPMG 2800 Army Pentagon, Washington DC 20310	HQDA OPMG
	11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

Project Leader: Serena Chan

14. ABSTRACT

The telecommunications industry is retiring its legacy switches, routers, and associated analog networks and replacing them with more capable and robust digital components based on Internet Protocol (IP) networking. Consequently, the suite of technologies underlying the way that first responder organizations, including those in the Army, currently receive, process, and respond to 9-1-1 calls will require migrating to an IP-based 9-1-1 environment, known as Next Generation 9-1-1 (NG911). Many states and local jurisdictions across the U.S. have already begun transitioning their public safety answering points to NG911, resulting in a burgeoning capability gap with the Army environment. This migration is critical, as installations that do not upgrade will become, at best, islands unable to share information with critical mission partners; at worst, they will become unable to process emergency requests for service at all. Thus, the Army requires a comprehensive, enterprise-wide strategy guiding the acquisition and deployment of NG911 capabilities.

15. SUBJECT TERMS

Next generation 9-1-1 (NG911), capability gap, Army, public safety communications

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Katherine Brennan
Unclassified	Unclassified	Unclassified	Unlimited	258	19b. TELEPHONE NUMBER (Include Area Code) 703-692-6721